Internetworking With CISCO Routers & Switches

Course Outline

- Intro to Routing
- Router Interfaces
- Cisco Discovery Protocol (CDP)
- Routing
  - Static Routes
  - Distance Vector Routing
  - Link State Routing
  - Dynamic Routing
- Security Issues
- Advanced Topics

Graphic Symbols

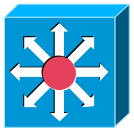

Bridge


Switch

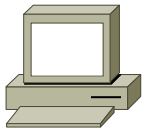

Router


Access server


ISDN switch

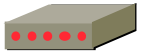

Multi-layer switch


Network switch


Personal computer

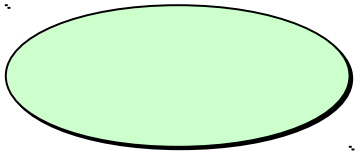

File Server

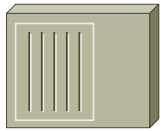
Data Service Unit/ Channel Service Unit

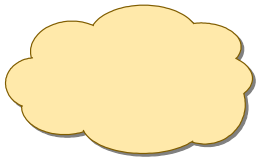

Modem

Web Server


WAN “cloud”


VLAN (Color May Vary)


Hub


Network Cloud or Broadcast Domain

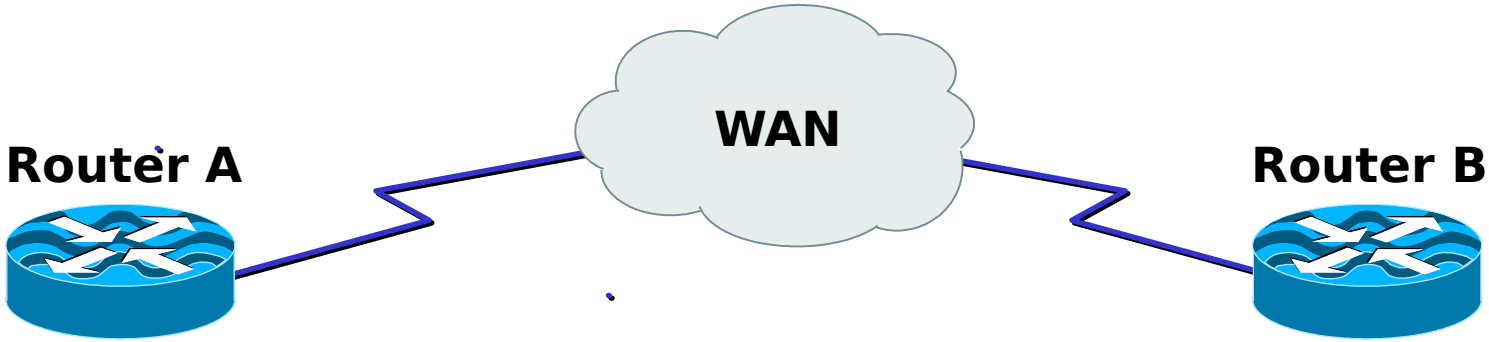
Ethernet


Fast Ethernet


Serial Line

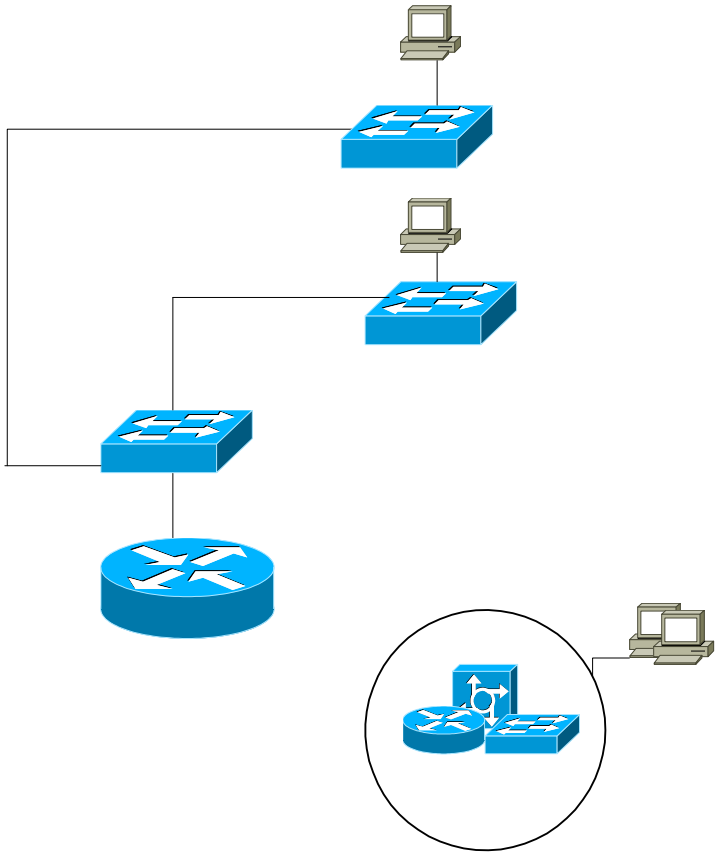

Circuit Switched Line

What do Routers do?



- Routers gather and maintain routing information to enable the transmission and reception of IP Datagrams
- Routing information is kept in a routing table
  - One entry for each known route
- Routers can create and maintain the routing table dynamically to accommodate network changes as they occur
- The rules for the exchange of routing information amongst routers are called routing protocols

What do Routers do?



- Broadcast Control
- Multicast protocol
- Optimal Path determination
- Traffic Management
- Connects to WAN services

- **How do they do this?**

Media Characteristics

MSTP

	IFG	Minimum Valid Frame	Maximum Valid Frame	Bandwidth
Ethernet	96 bits	64 Bytes	1,518 Bytes	10 Mbps
Fast Ethernet	96 bits	64 Bytes	1,518 Bytes	100 Mbps
FDDI	0	34 Bytes	4,500 Bytes	100 Mbps
Token Ring	4 bit	32 Bytes	16K Bytes	16 Mbps
BRI	0	24 Bytes	1500 Bytes	128 Kbps
PRI	0	24 Bytes	1500 Bytes	1.472 Mbps
T1	0	14 Bytes	4500 Bytes	1.5 Mbps
ATM	0	30 Bytes (AAL5)	16K Bytes (AAL5)	155 Mbps

LAN Interfaces: Broadcast and Multicast Traffic

- What's so bad about broadcasts?
  - Consume network bandwidth
  - Consume host station CPU capacity
- Sources of broadcast/multicast traffic
  - Clients looking for services
    - Apple Talk, Netware, Net BIOS, and TCP/IP clients
  - Servers announcing services
  - Routing protocol updates
  - Bridge Protocol Data Unit (BPDU) Frames
  - Forwarded by bridges and switches

LAN Interfaces:Broadcast and Multicast Traffic

- Controlling broadcast/multicast traffic
  - Rule of thumb:<20% broadcasts/multicasts per segment
  - Can be calculated with (# broadcasts)/(# packets input)
  - Limit maximum number of stations per segment
  - Guidelines

Ethernet: Performance Issues

- Measuring network utilization
  - Protocol analyzers
  - User complaints
  - Rule of thumb: shared Ethernet segments <40% utilization
- Improving network utilization
  - Segmenting with routers
  - Segmenting with switches

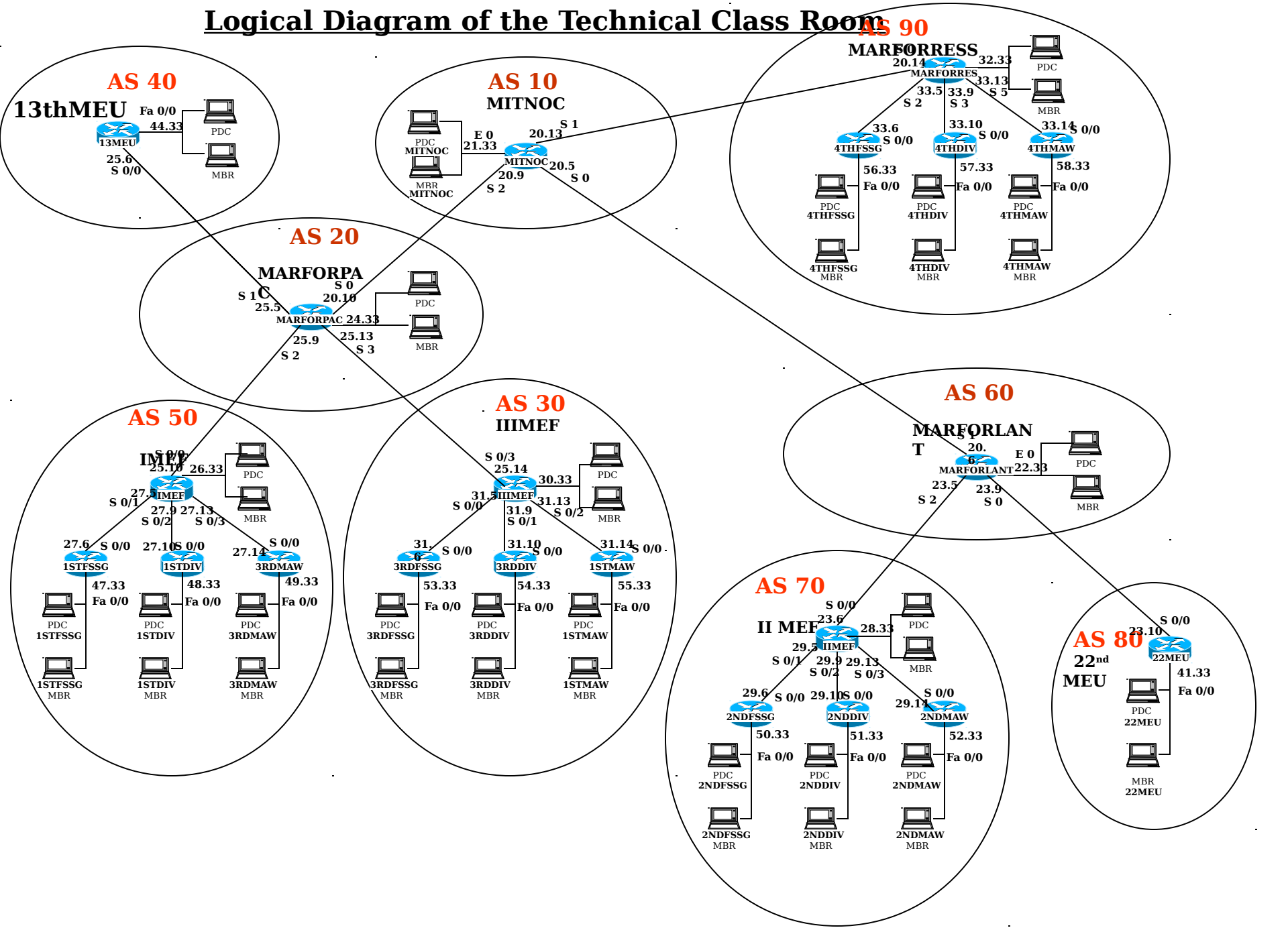
Routing

- Connected, Static, Default
- Distance Vector, Link-State
- Dynamic

IP Routing

- Routers learn routes by:
  - Directly connected networks
  - Routing information exchange with other routers
  - Static routes
- Default router
  - Every host should have a default router defined
  - ***Default router must be reachable

Logical Diagram of the Technical Class Room

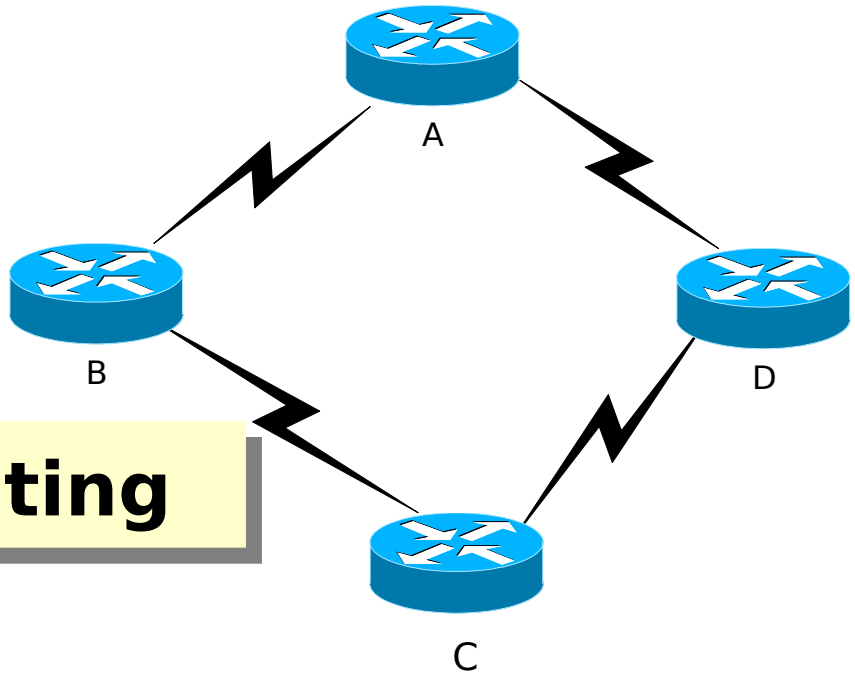


Routing Protocols

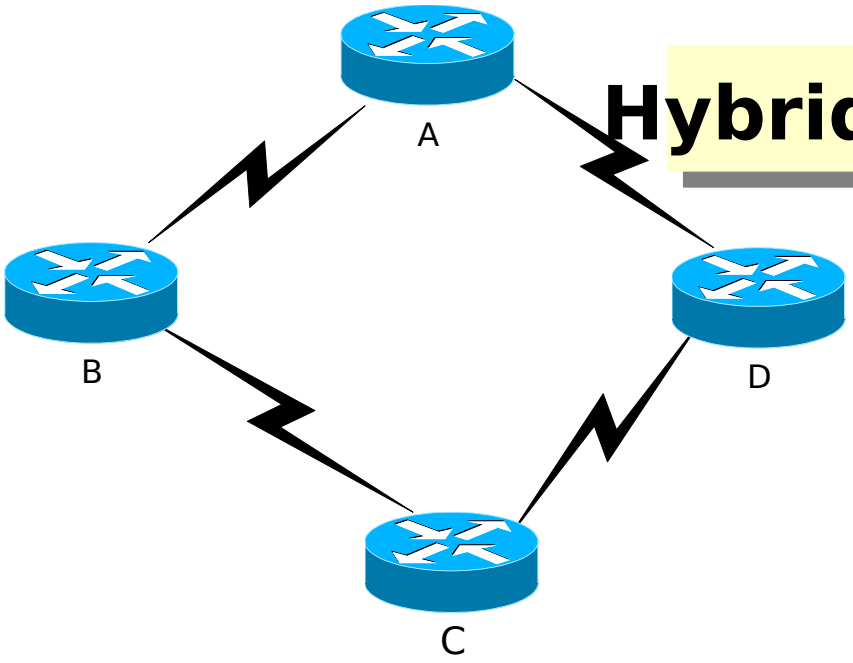
- Determine the "best" route to each destination network
- Distribute routing information amongst systems
- Distribute reach ability information amongst systems
- Interior routing protocol
  - Interior to an autonomous system
  - Under a common administration
  - Chosen by autonomous system's administrator
- Exterior routing protocol
  - Between autonomous systems
  - Not under a common administrator

Classes of Routing Protocols

Distance Vector



Hybrid Routing



Link State

Which Protocol?

- **Issue: Time to Convergence**

Convergence occurs when all routers use a consistent perspective of network topology

After a topology change, routers must recompute routes, which disrupts routing

The process and time required for router reconvergence varies in routing protocols

Distance Vector vs. Link-State

Distance Vector	Link-State
• Views net topology from neighbor's perspective • Adds hop count value • Frequent, periodic updates: slow convergence • Passes copies of routing table to neighbor routers	• Gets common view of entire network topology • Calculates shortest path to other routers • Event-triggered updates: faster convergence • Passes link-state routing updates to the other routers

What is Best? It Depends

MSTP

Issues	Concern	Example Questions
Technical	Performance to meet specific needs	Metrics adequate for network size? Any load sharing?
Business	Conformity with enterprise policies and priorities	Proven technology? Multi-vendor support? Standards based?
Operational	Simplicity of network setup and management	Easy to configure? Able to handle several routed protocols?

th routing protocols, no one type fits all networks

Hybrid Routing

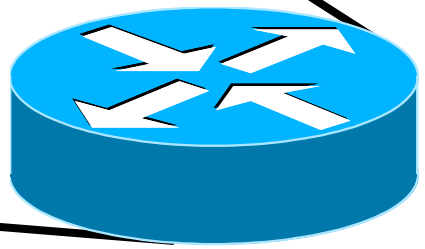
MSTP

Choose a routing path based on distance vectors

Balanced Hybrid Routing

Converge rapidly using changed-based updates

Share attributes of both distance-vector and link-state routing



Autonomous System

- An autonomous system is a collection of networks under a common administration sharing a common routing strategy. An autonomous system may comprise of one or many networks, and each network may or may not have an internal structure (subnetting).
- The AS number, which is assigned by the NIC, is a 16-bit decimal number that is uniquely assigned.
- An assigned AS is required in order to run BGP, IGRP, or EIGRP.

Interior Routing Protocols

- EIGRP (Enhanced Interior Gateway Routing Protocol)
  - developed by Cisco
  - distance vector
  - sends out only updates when they happen vice whole tables every 30 seconds
  - supports VLSM
  - from global configuration

  HOSTNAME(conf)#router eigrp [*AS*]

  HOSTNAME(conf-router)#network [*ip network*]

Requirements for an Internet Routing Protocol

The protocol must be:

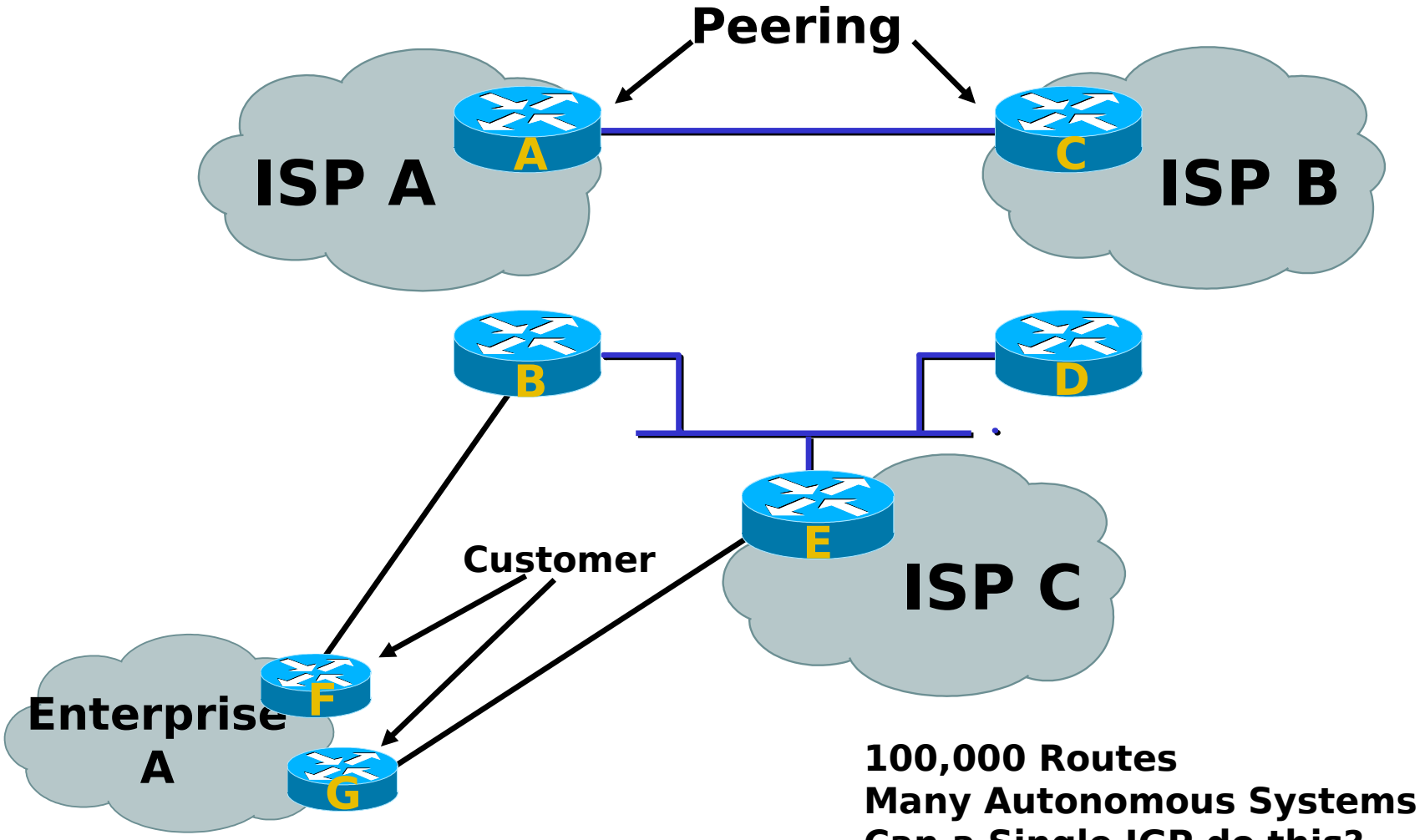
Scalable

Stable

Flexible

…BGP is <u>this</u> Protocol

BGP Basics



100,000 Routes
Many Autonomous Systems
Can a Single IGP do this?

Reasons for Using BGP

- 1: You need to scale your IGP
- 2: You're a multi-homed ISP customer and need to implement routing policy
- 3: You need to transit full Internet routes

Interior Vs. Exterior Routing

- Interior
  - Automatic discovery
  - Generally trust your IGP routers
  - Routes go to all IGP routers
- Exterior
  - Specifically configured peers
  - Connecting with outside networks
  - Set administrative boundaries

Why Do We Need an EGP?

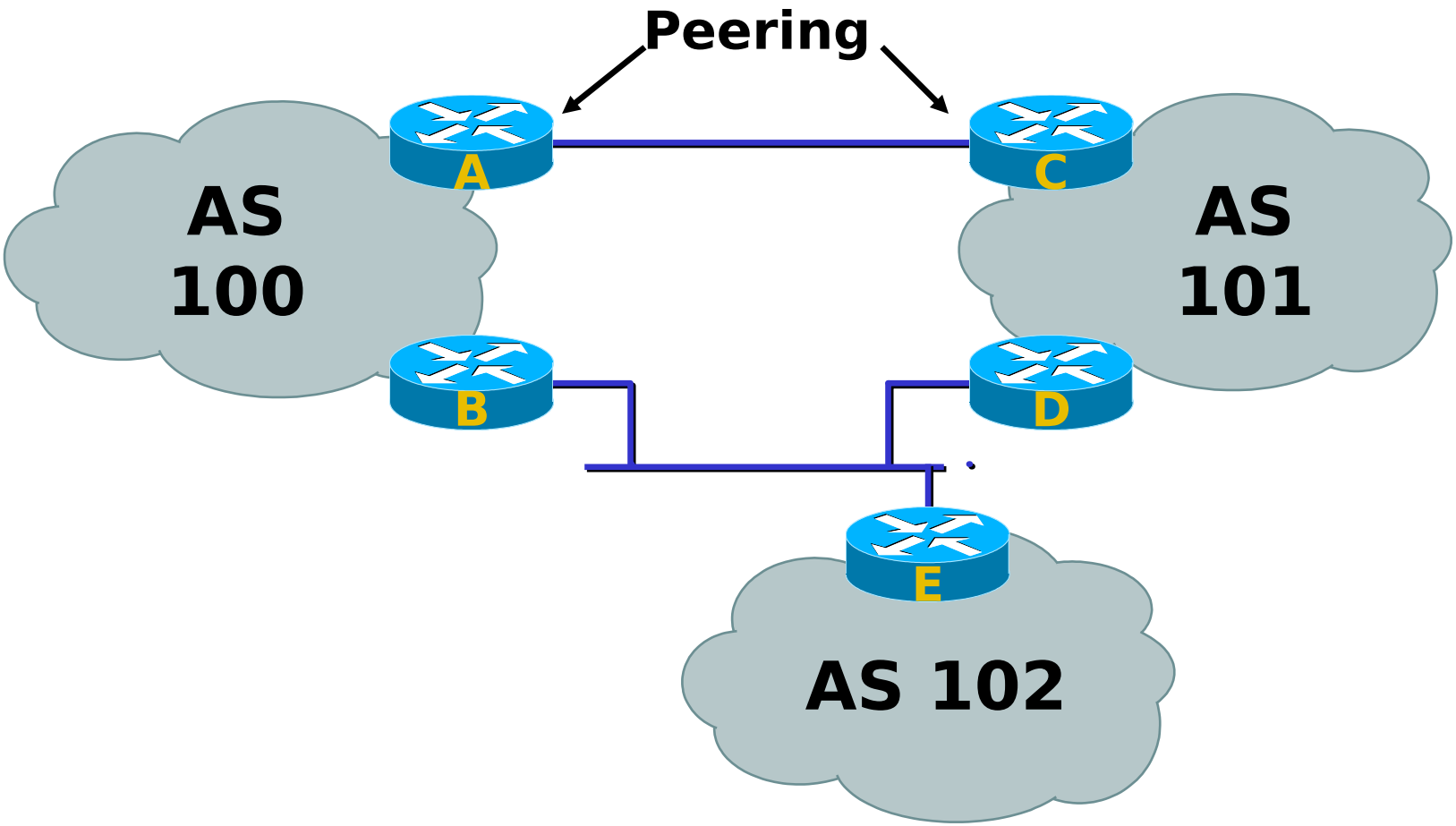
- Scaling a large network—"Divide and Conquer"
  - Hierarchy
  - Periodic IGPs/Flooding
  - Isolate network stability
- Complex Policies
  - Control reachability to prefixes
  - Merge separate organizations
  - Connect multiple IGPs

Concept of Autonomous System

MSTP

- A network(s) sharing the same routing policy
  - Possibly multiple IGPs
  - Usually under single administrative control
- Contiguous internal connectivity
- Numbering range form 1 to 65,535—globally unique—“AS Number”
  - Private range: 64512–65535

IGP of Each AS Is Hidden



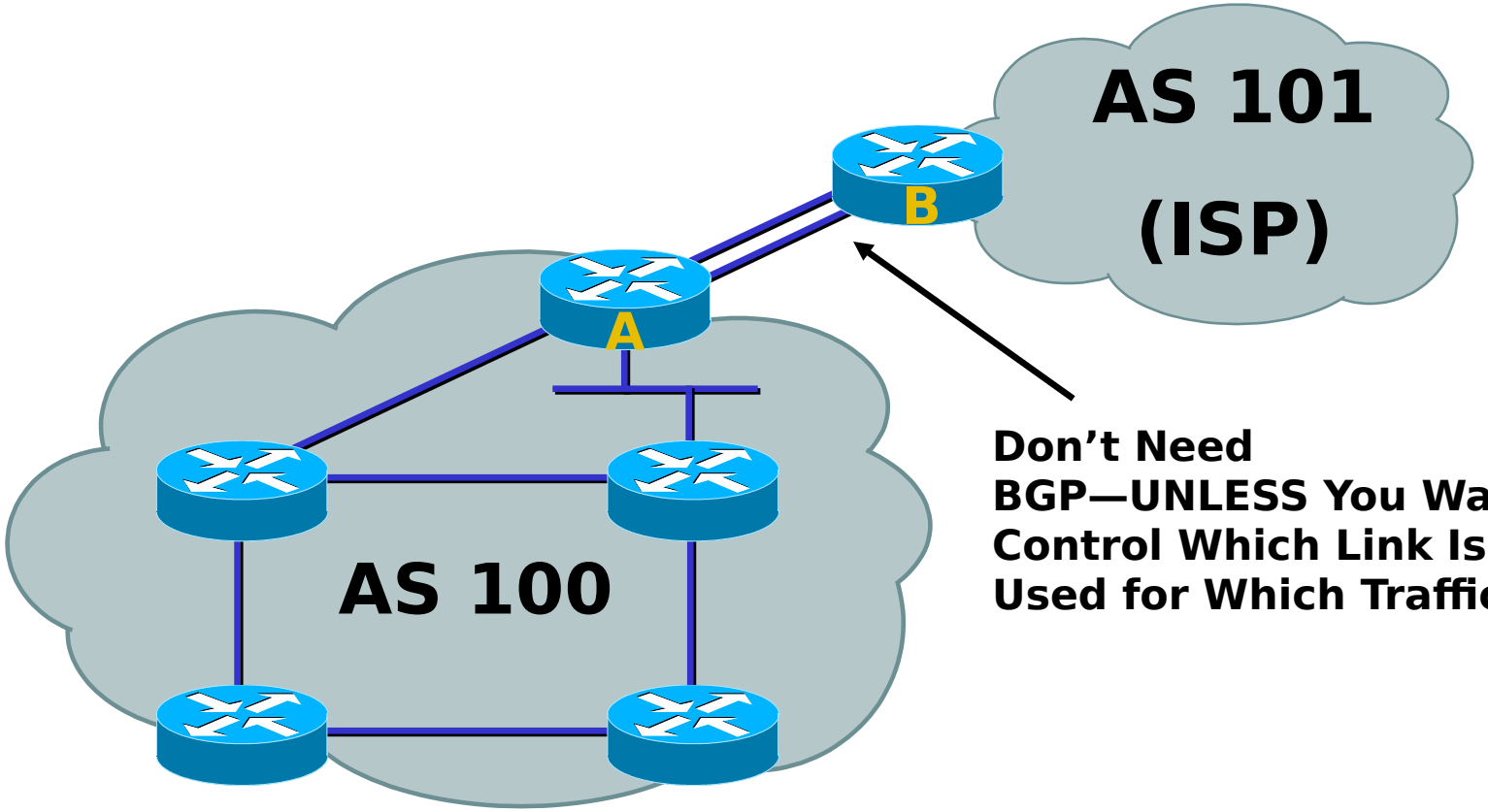
Reasons for Using BGP

- 1: You need to scale your IGP
- 2: You're a multi-homed ISP customer and need to implement routing policy
- 3: You need to transit full Internet routes

Stub Network

- No need for BGP
  - ISP advertises the stub network
  - Policy confined within ISP policy
- Default to the border

Stub Network

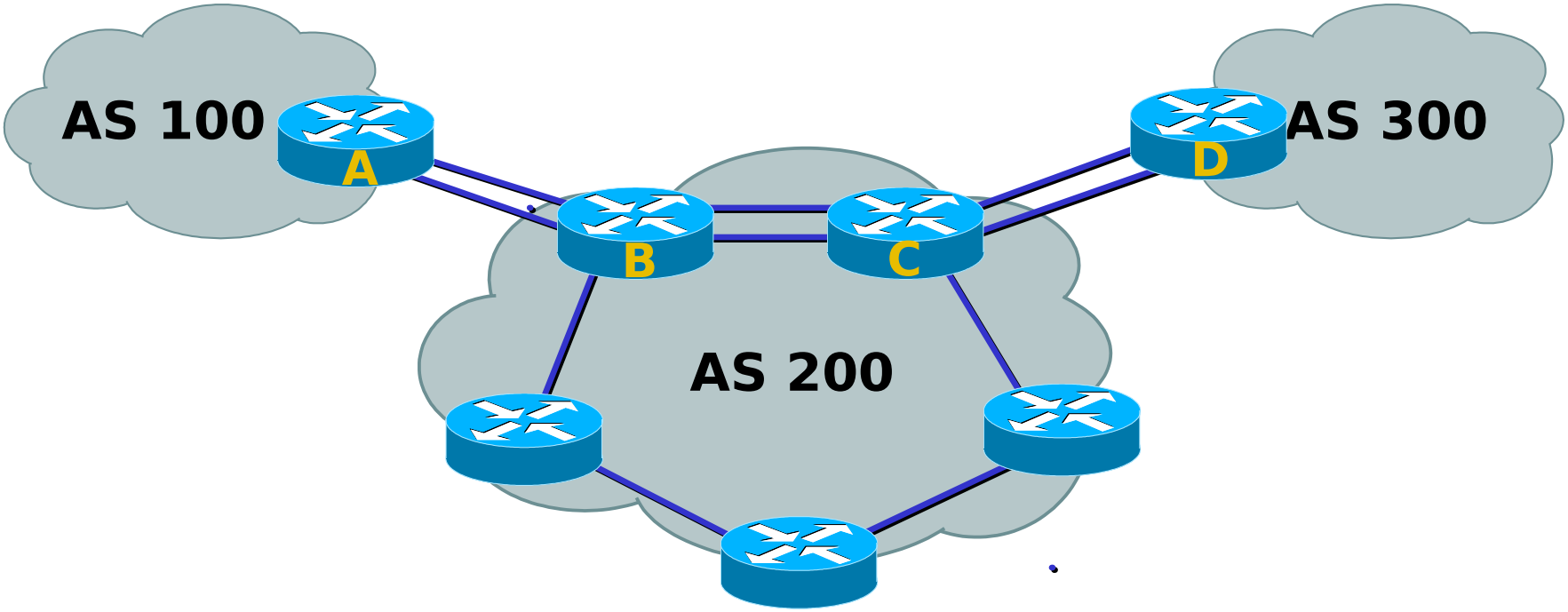


Don’t Need BGP—UNLESS You Want to Control Which Link Is Used for Which Traffic

Multi-Homed Network

- Many situations possible
  - Multiple links to same ISP—without BGP
  - Secondary for only backup—without BGP
  - Loadshare between primary and secondary— without BGP
  - Selectively use different ISPs—need BGP

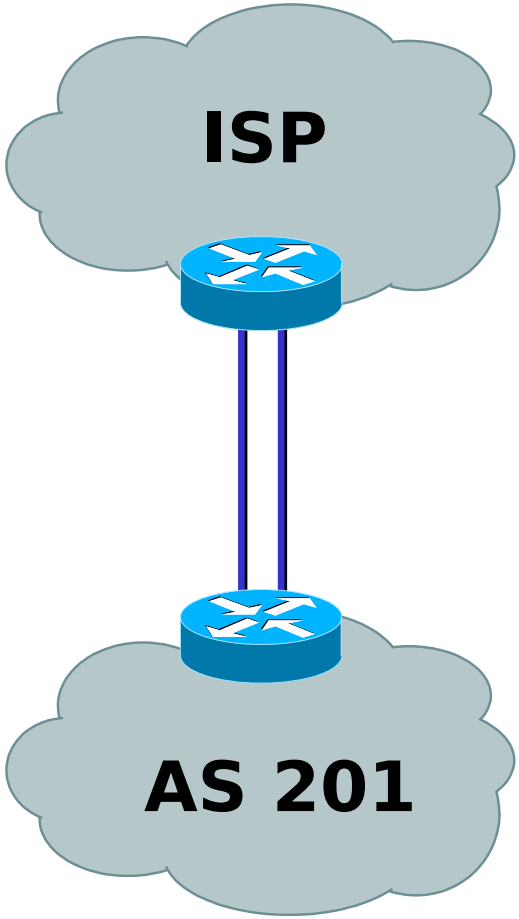
Multi-Homed Network



Can Still Use Default, UNLESS You Want to Selectively Use Either ISP for Optimal Performance

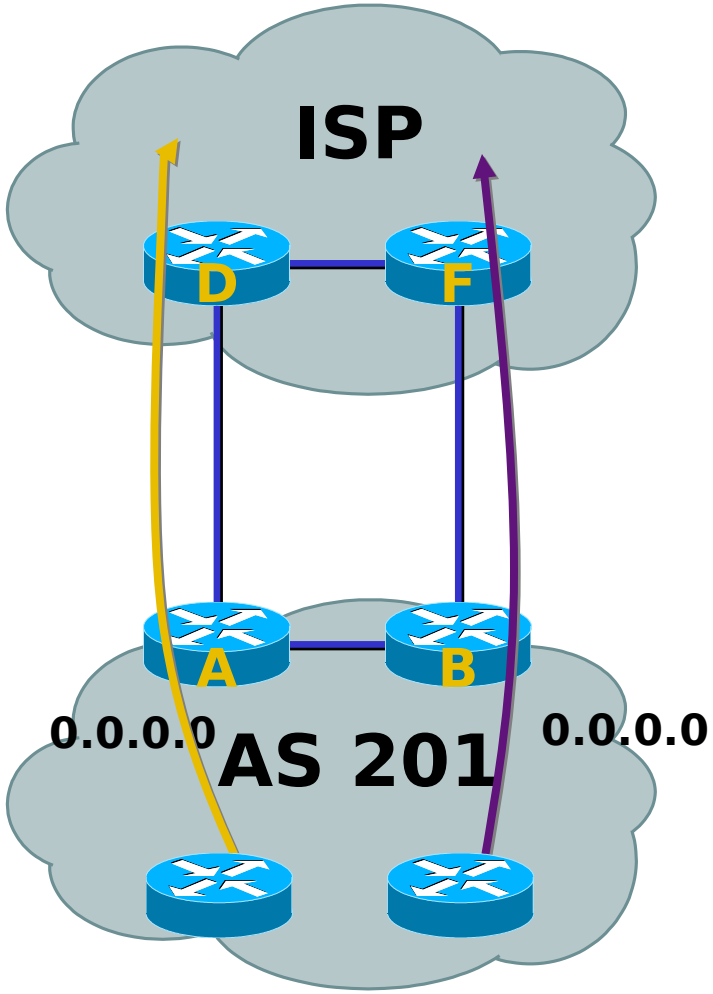
Multiple Links to the Same ISP I

- Can still use default for outbound routing
- For inbound routing:
  - –Option1: ISP can use floating statics, or IGP to learn your routes and loadshare
  - –Option2: Can use BGP to loadshare



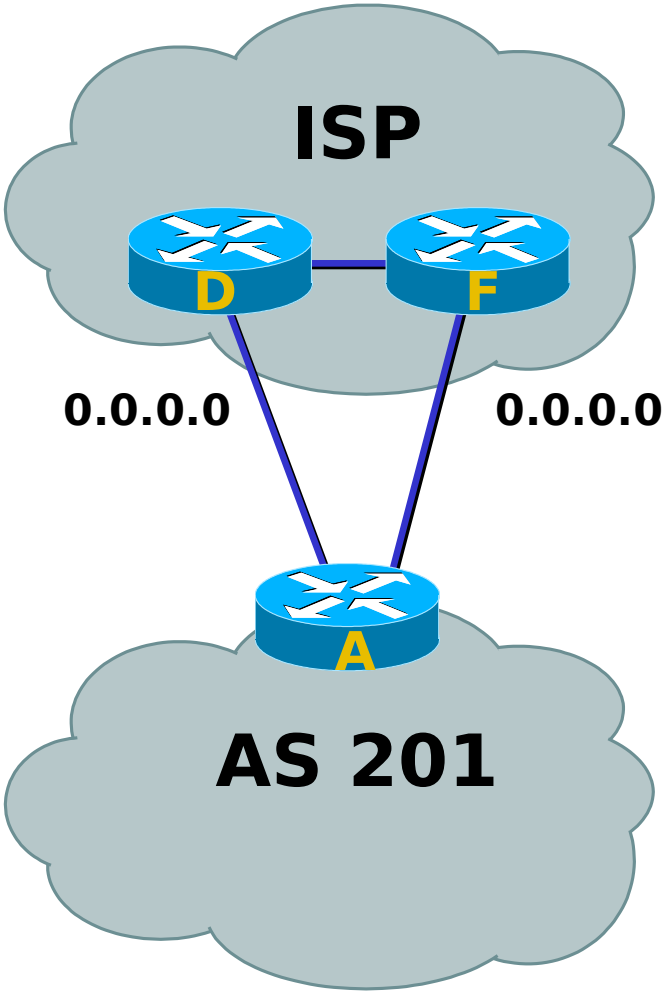
Multiple Links to the Same ISP II

- Simplest scheme is to use two defaults
- Again, can use statics/IGP at borders, or use BGP

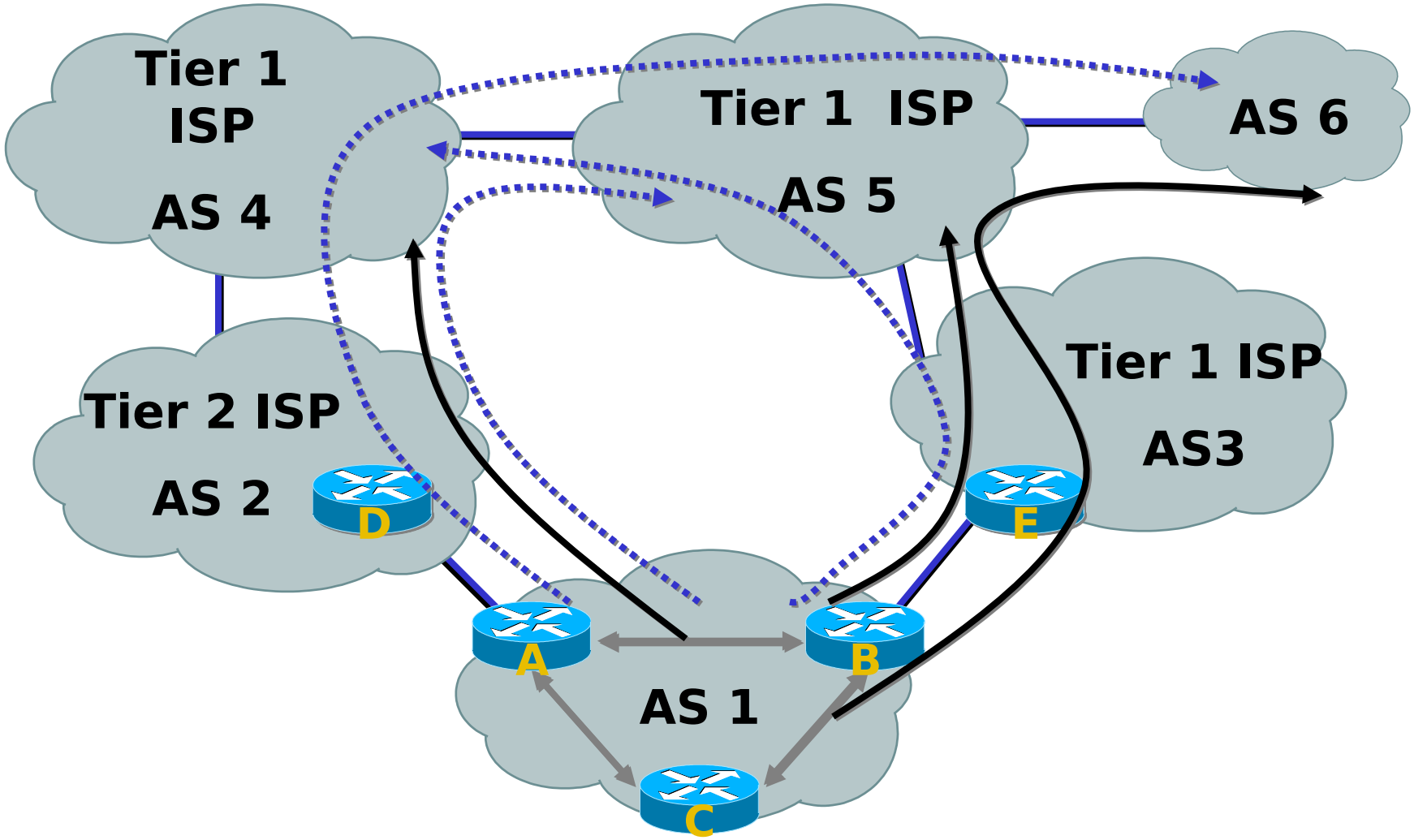


Multiple Links to the Same ISP III

- Again, can just use two equal cost defaults to reach ISP
- Statics/IGP OR BGP to advertise your routes to ISP



Why Use BGP for Multi-Homing?

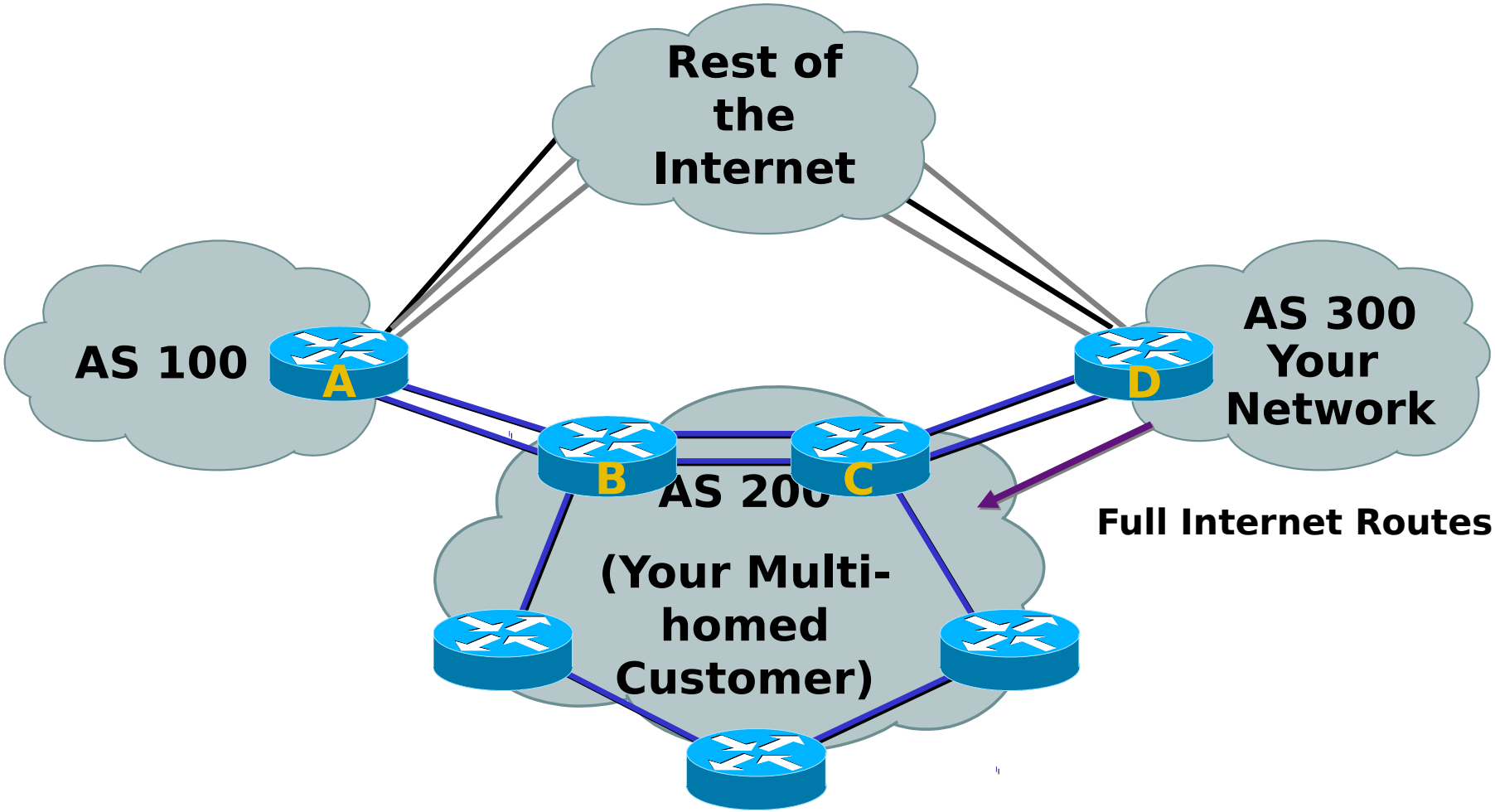


Reasons for Using BGP

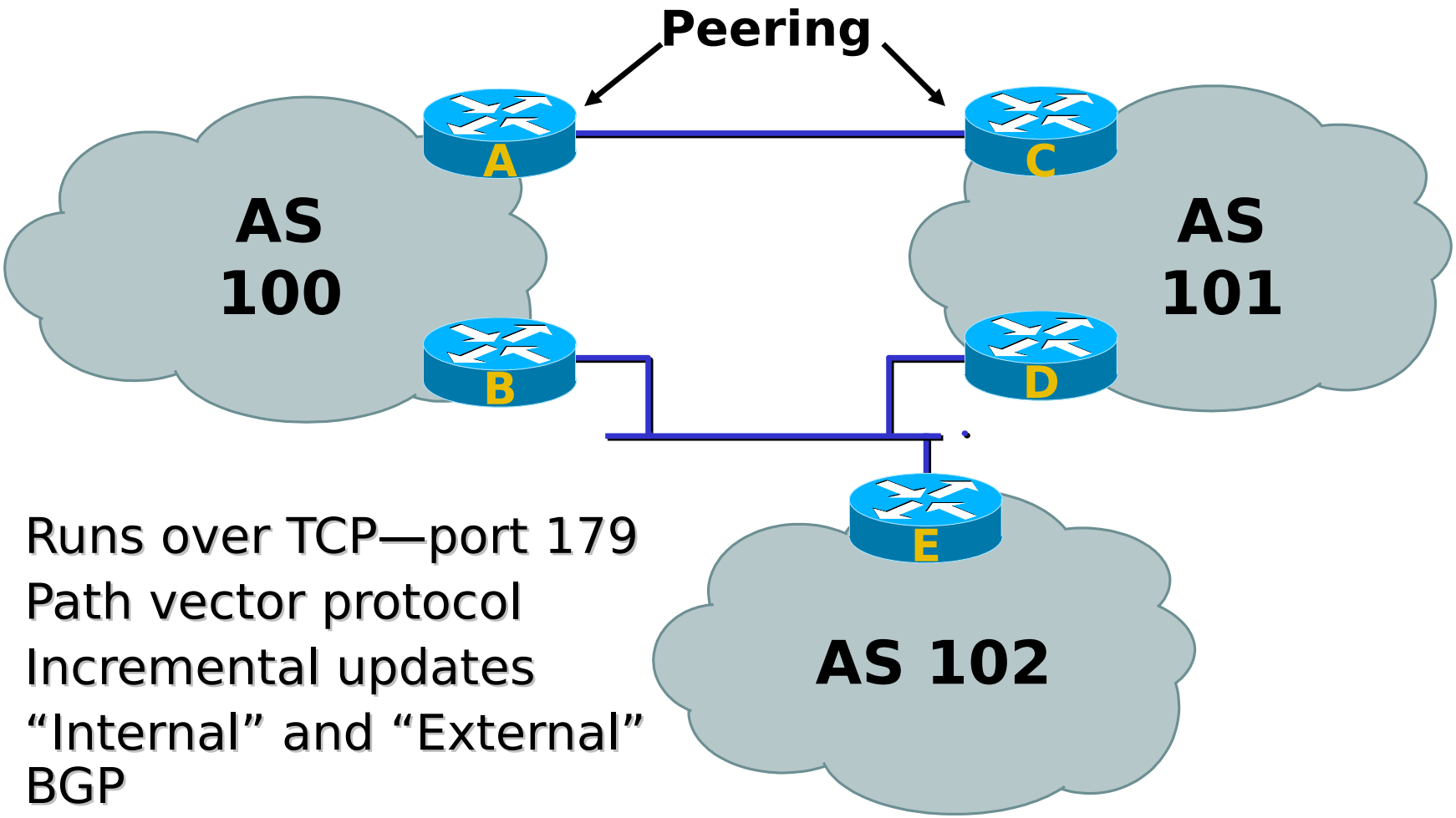
- You need to scale your IGP
- You're a multi-homed ISP customer and need to implement routing policy
- You need to transit full Internet routes

You Need to Transit Internet Routes

(ie, You are an ISP)



Back to Basics



- Runs over TCP—port 179
- Path vector protocol
- Incremental updates
- “Internal” and “External” BGP

General Operation

- Learns multiple paths via internal and external BGP speakers
- Picks THE bestpath, installs it in the IP forwarding table, forwards to EBGP neighbors (not IBGP)
- Policies applied by influencing the bestpath selection

Summary of Operation

- TCP connection established (port 179)
- Both peers attempt to connect—there is an algorithm to resolve “connection collisions”
- Exchange messages to open and confirm the connection parameters
- Initial exchange of entire table
- Incremental updates after initial exchange
- Keep alive messages exchanged when there no updates

Configuring Exterior Routing

- Configuring exterior routing protocols requires three sets of information.
  - A list of neighbor (or peer) routers with which to exchange routing information. This list is created with the neighbor router subcommand
  - A list of networks to advertise as directly reachable, created with the network router subcommand.
  - The AS number of the local router.
- Example BGP Configuration (> ver 4)
  - router bgp 110 (your local AS #)
    network 131.108.0.0 (network you wish to advertise)
    neighbor 131.108.100.2 remote-as 109 (IP of router in AS 109)

Default Routing

- Manually configuring a static

```
R1# (config) ip route 0.0.0.0 0.0.0.0 192.168.10.1
```

- Source a default route via IGP
  - Define a static route on one router
  - Redistribute static route into IGP

```
R1# (config) #ip route 0.0.0.0 0.0.0.0 192.168.10.1
R1# (config) #router rip
R1# (config-router) #redistribute static
```

- Specifying a default network
  - IGP will decide “best” route to default network

```
R1# (config) #ip default-network network-number
```

Redistributing Data

- Redistributing is the concept of passing unlike protocol information through different routing protocols. An example is IGRP will talk to all other IGRP clients, if you wish to also let those IGRP clients know about the manually added static routes on a router you would enter redistribute static as a router subcommand under the IGRP definition.

ip route 192.1.2.0 192.31.7.65 (static route)

ip route 193.62.5.24 255.255.255.248 192.31.7.65 (static route)

router igrp 110 (shares routing information with AS 110)

network 192.31.7.0 (locally connected network)

redistribute static (passes the two static routes as well)

redistribute rip (pass all RIP learned

Default Metric

The following example takes redistributed RIP metrics and translates them into EIGRP metrics with values as follows:

bandwidth = 1000
delay = 100
reliability = 250
loading = 100
mtu =1500

router eigrp 109
network 131.108.0.0
redistribute rip
default-metric 1000 100 250 100 1500

Routing Protocol Weights

The weight of a protocol helps the router to decide which is the

Directly Connected	0
Static	1
BGP (external)	20
EIGRP (internal)	90
IGRP	100
OSPF	110
RIP	120
EGP	140
EIGRP (external)	170
BGP (internal)	200
Unknown	255

Security Issues

- Password Security
- Keeping Out Unwanted Guests
- Allowing Certain Information

Passwords

MSTP

- Enable
  - *Enable password {password}*
- Enable Secret
  - Enable secret {*password}*
- VTY
  - Line vty 0 4
  - Login
  - Password {*password}*
- Aux and Console
  - Line Con 0 (Aux 0)
  - Login
  - Password *{password}*

Password Security

- Password security is crucial for network integrity. It is recommended to mix the cases of the letters, and using "special characters" also helps in warding off hackers. Example: 2b,OR#2b.
- Never keep copies of configurations laying around that still display the passwords. Always edit the file after loading it onto a local drive.
- Outside administrators can still view most information without needing to know the Enable password. Always offer just a terminal login password unless they need to reconfigure as well.

Cisco Banners

- MOTD – Message of the Day
  - Router#banner motd #
    Stop! Government site
    #
- Incoming
- Exec
- Login

Access Lists

- Access Lists determine what type of traffic is or is not allowed to travel through certain ports.
- Several Access Groups can be made to allow for different settings for particular ports or groups of ports.
- Some basic rules of access lists:
  - access commands are dependent on order of entry
  - if a packet meets any condition it is approved, else it is denied and is not sent out the port.
  - restrictions can be set to either incoming or outgoing traffic. Be sure to set the lists in the right direction.
  - It is usually best to use reverse logic for restrictions. That is to say, restrict all traffic, then set what is allowed.

Advance Topics

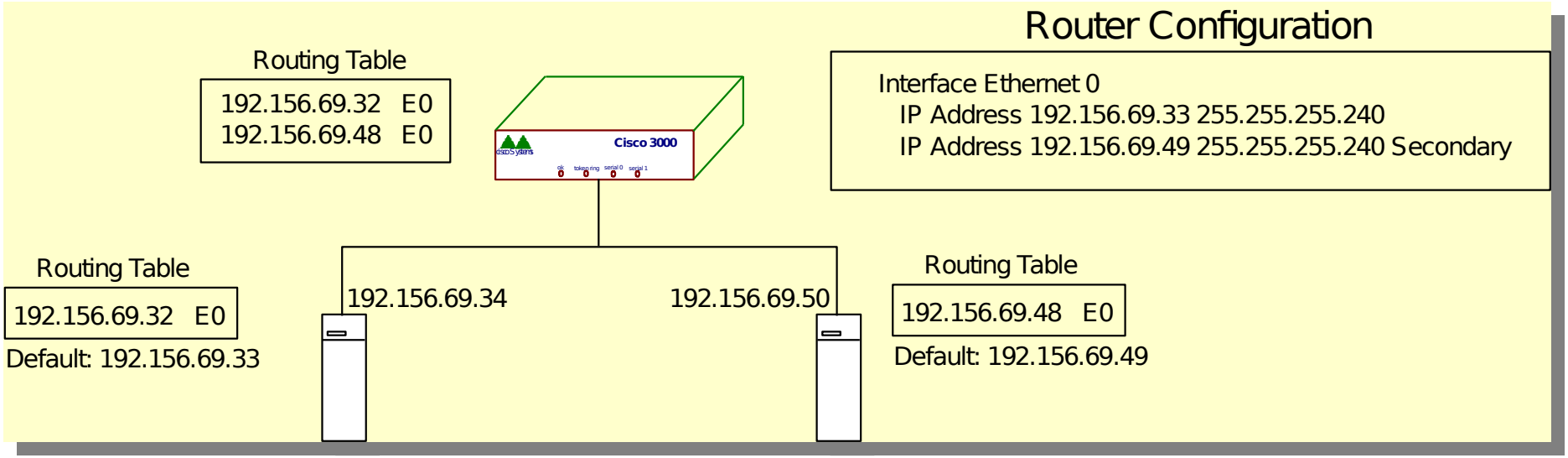
- Secondary Addresses
- Collapsing Backbones
- CIDR/Supernetting
- VLSM
- Queuing

Multiple Networks On The Same Line

- Should only be used when migrating
- Benefits
  - Allows for easy migrations
  - Works well for systems that use the broadcast address to advertise to clients, such as GCCS.
- Costs
  - Very inefficient at routing

Multiple Networks On The Same Line

- Trace the network traffic between devices:
- Both workstations work fine when sending traffic to the router (default).
- When sending to each other, each workstation sends the traffic to the router first because the other workstation is not a known network.

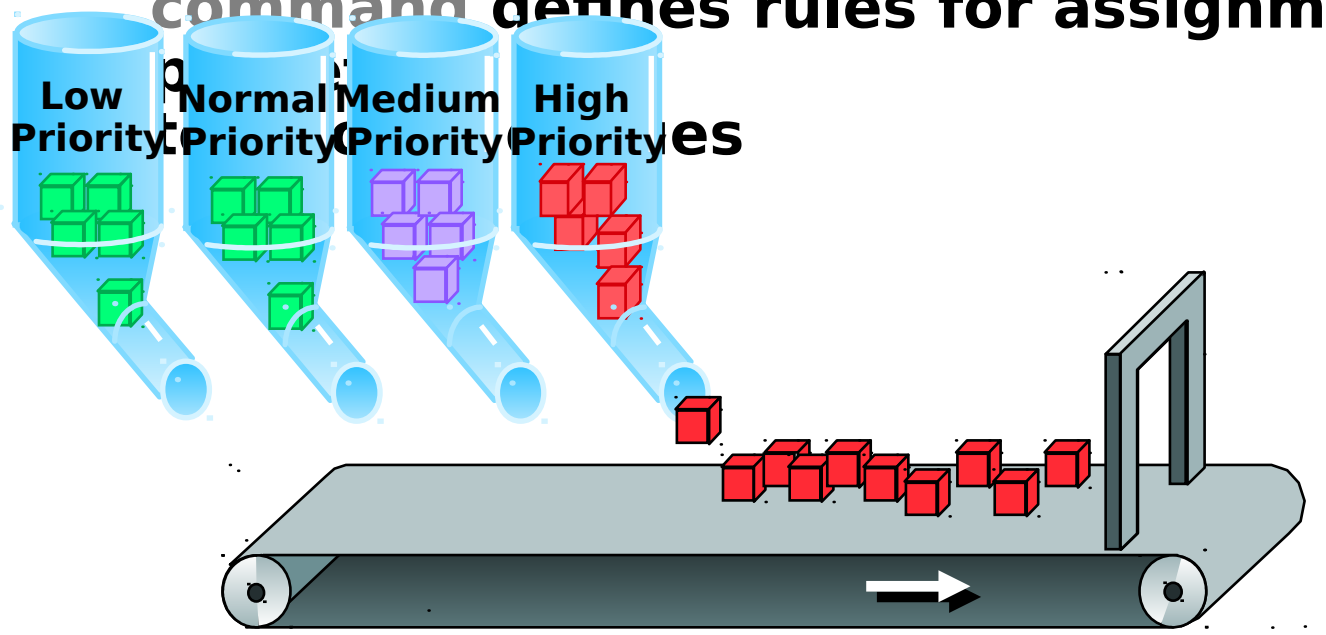


Queuing

- The Cisco IOS implements four (now five) different queuing algorithms today:
  - First in, First Out (FIFO) Queuing
  - Priority Queuing
  - Custom Queuing
  - Weighted Fair Queuing
  - Interleave with Fragmentation
- Queuing occurs when network congestion occurs (i.e., the queue depth => 1), else all packets are sent as they arrive at the interface

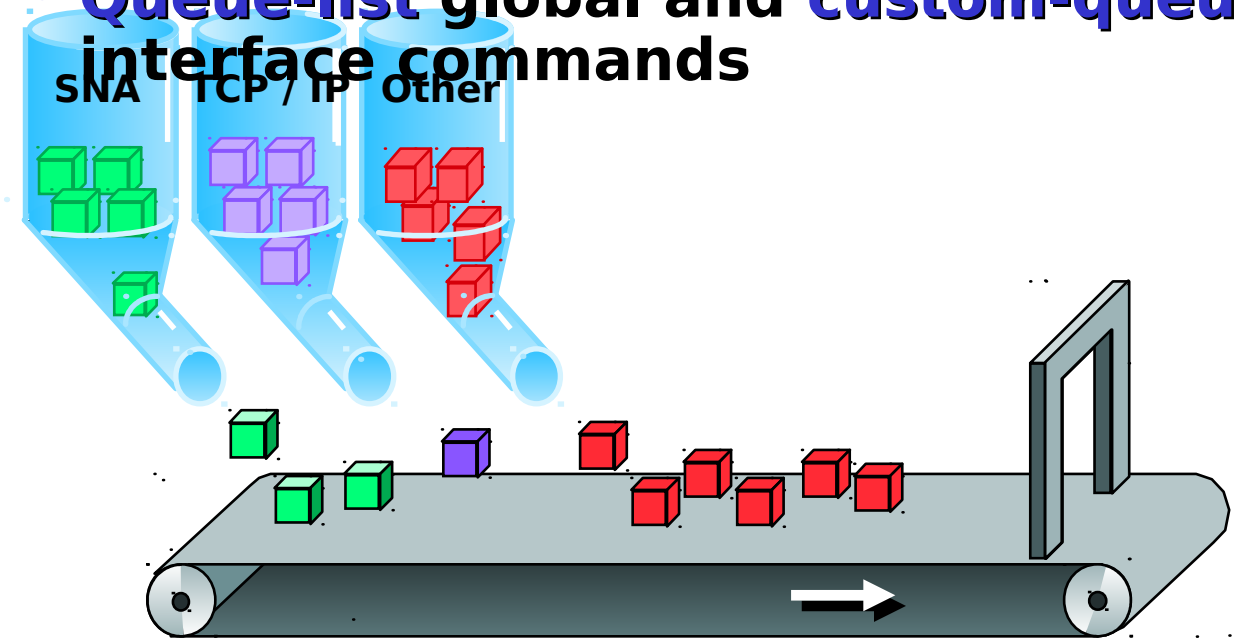
Priority Queuing

- **Four queues: high, medium, normal and low**
- **Priority-list global and priority-group interface command defines rules for assignment of packets to queues**



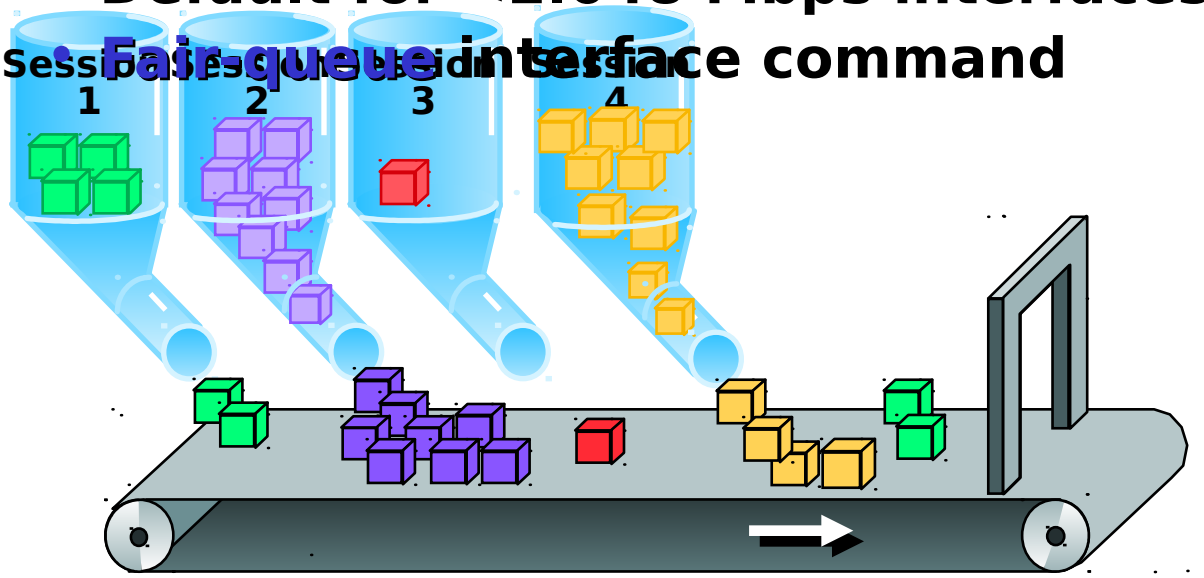
Custom Queuing

- **Control % of interface bandwidth for specified traffic**
- **17 output queues for each interface [16 configurable]**
- **Queue-list global and custom-queue-list interface commands**



Weighted Fair Queuing

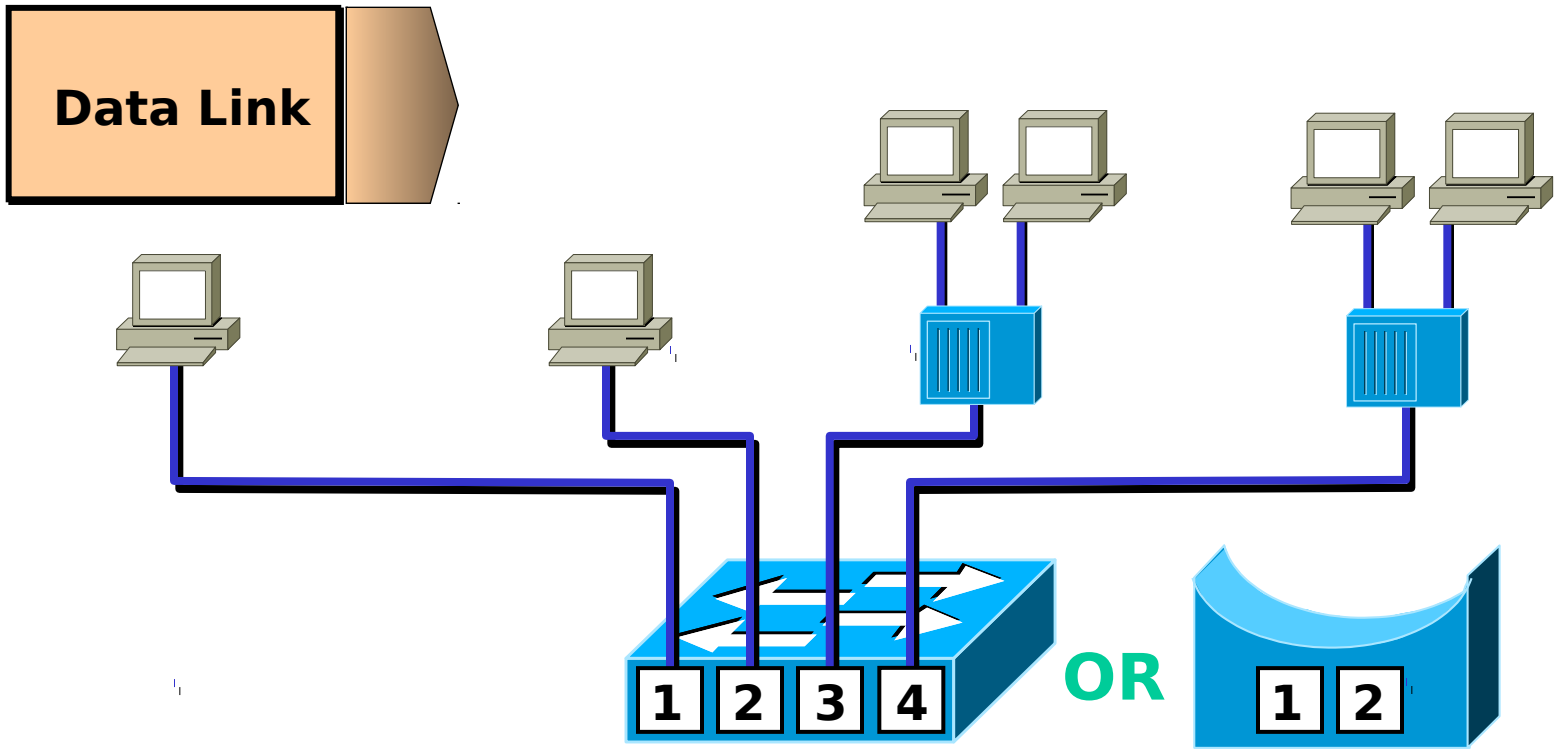
- **Automatic traffic priority management**
- **Low-bandwidth sessions have priority over high-bandwidth sessions**
- **High-bandwidth sessions assigned weights**
- **Default for <2.048 Mbps interfaces**
- **Fair-queue interface command**



IOS Requirements

- Certain features may require specific IOS versions. i.e. QoS, IOS Telephony Service, etc
- Should be standard across the MEF. (Be aware of platform limitations! i.e. memory)

Switches, Bridges, & Hubs

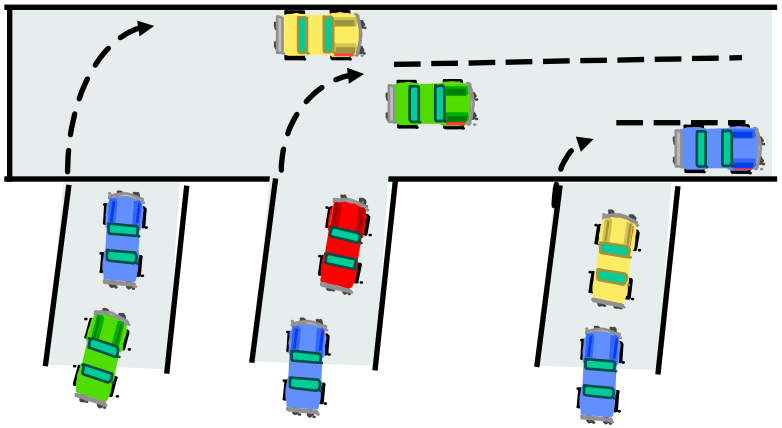


- Each segment has its own collision domain
- All segments are in the same broadcast do

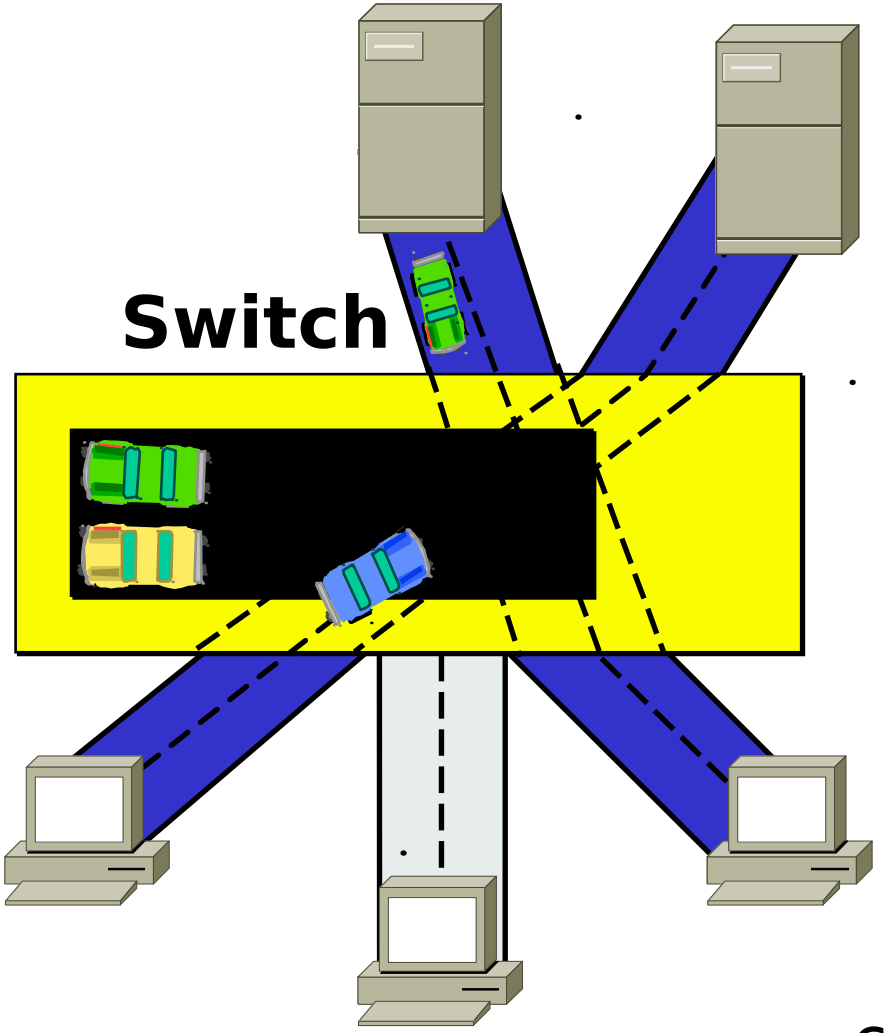
Ethernet: Collisions

- A certain level of collisions are expected on CSMA/CD LANs
- Excessive collisions can result from faulty components or overloaded segments
  - **Bad or excessively long cables**
  - **Bad NICs or transceivers**
- Establishing a baseline is helpful to determine normal levels
- Collisions produce fragments that are <64 size of frame
- Local collisions
  - **Occur on local LAN segment**
  - **Detected by circuitry in LAN interfaces**
- Remote collisions

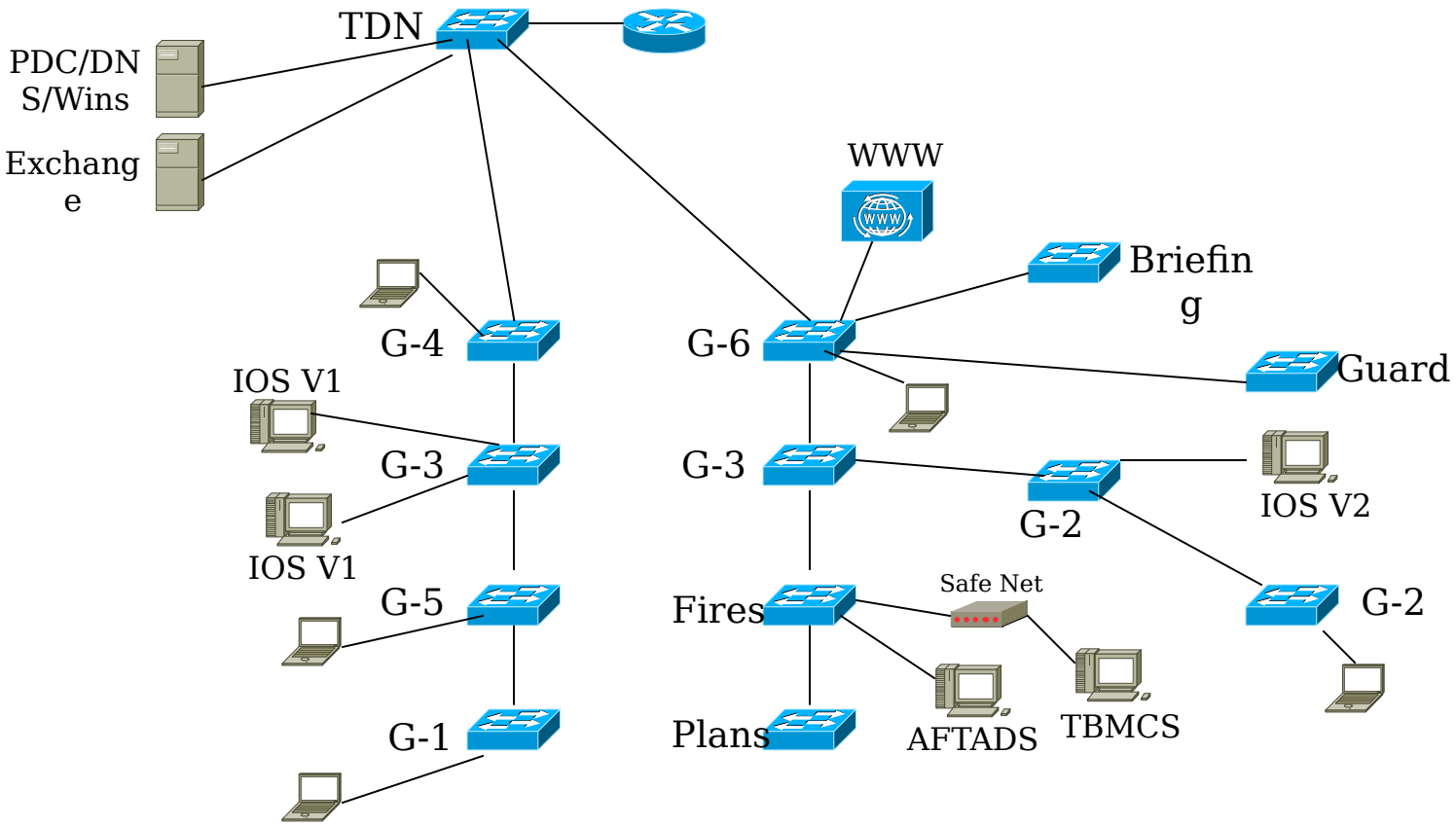
Advantage of Switches



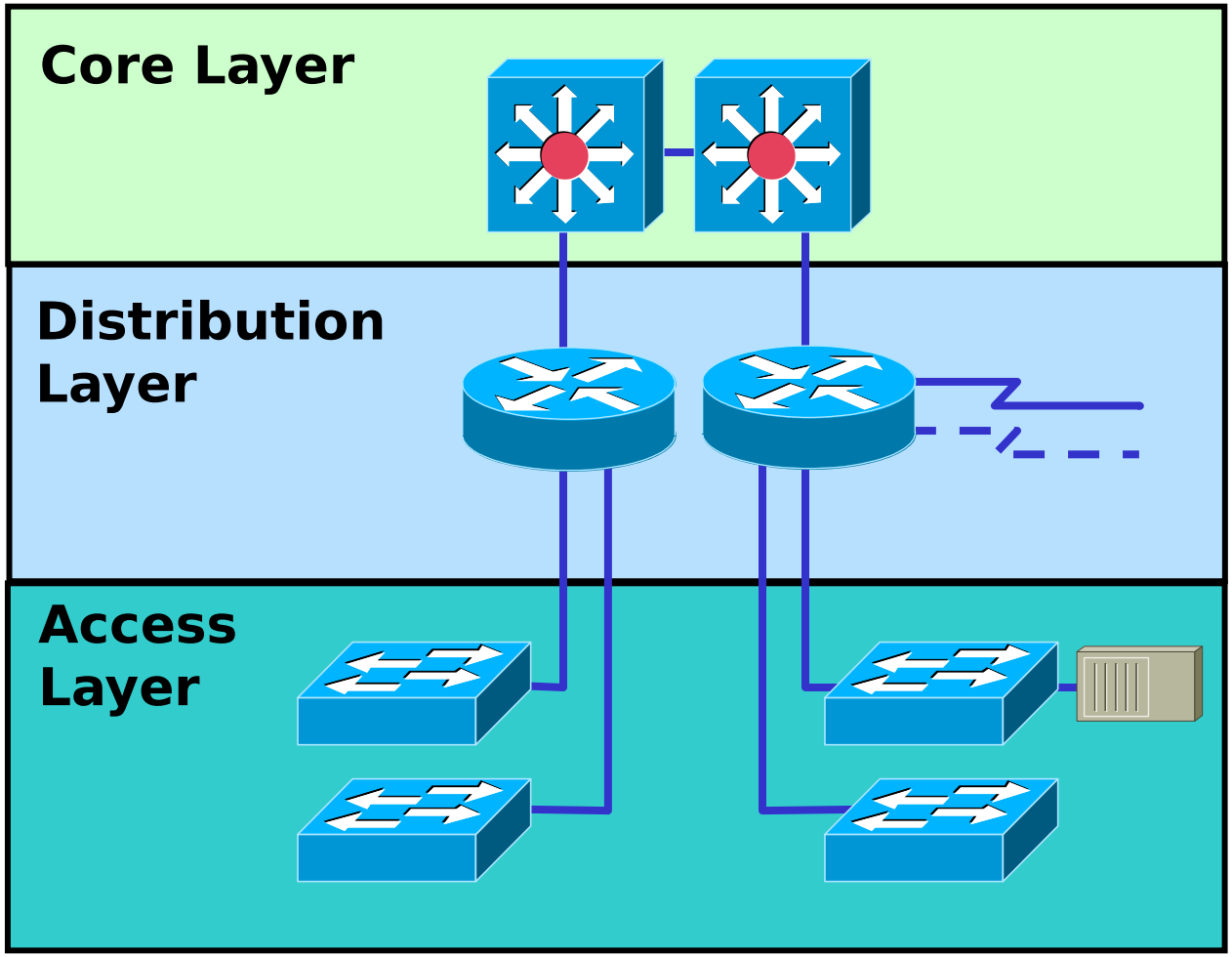
- **Each segment has its own collision domain**
- **Broadcasts are forwarded to all segments**



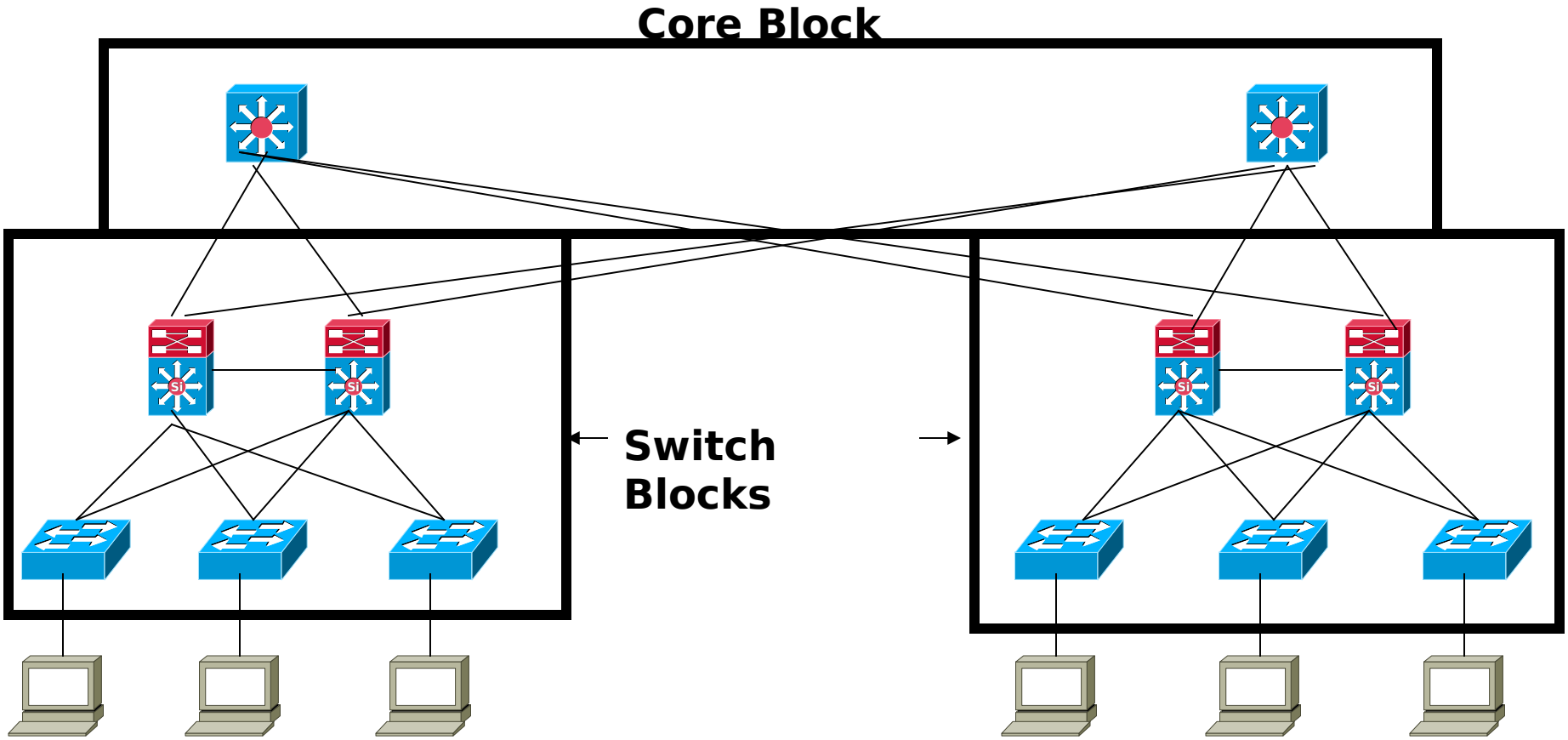
Switching Requirement



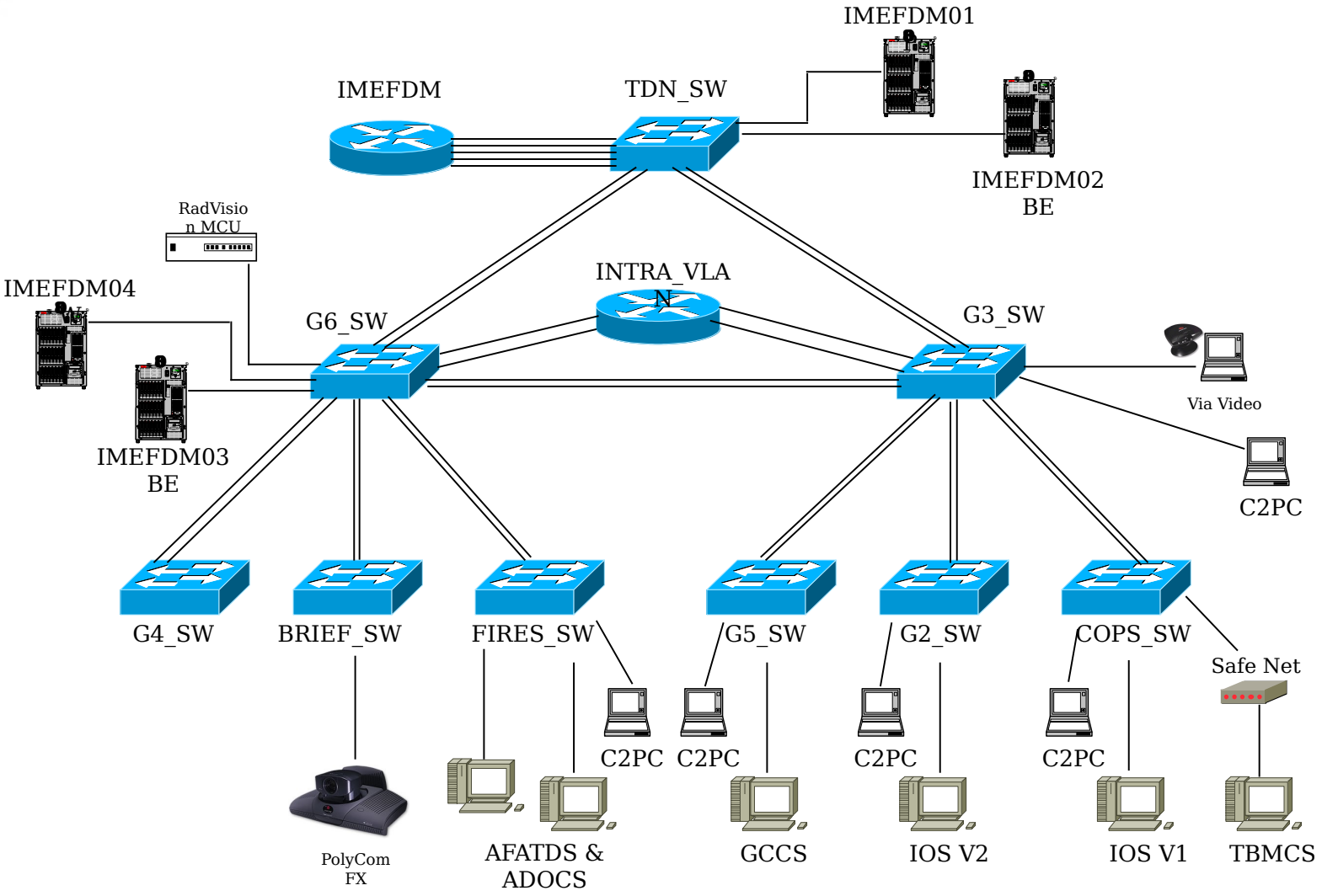
Cisco's Network Hierarchy



Building Block Method



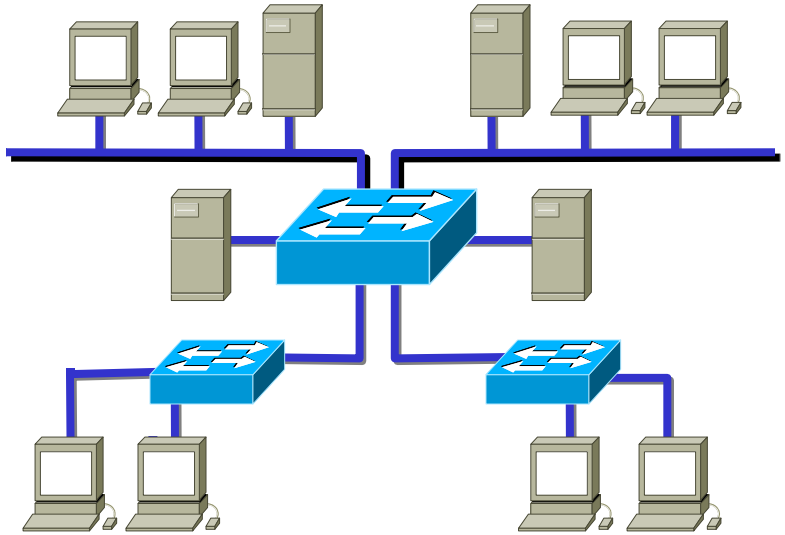
Switching Design (C2 Systems)



Switch Functions

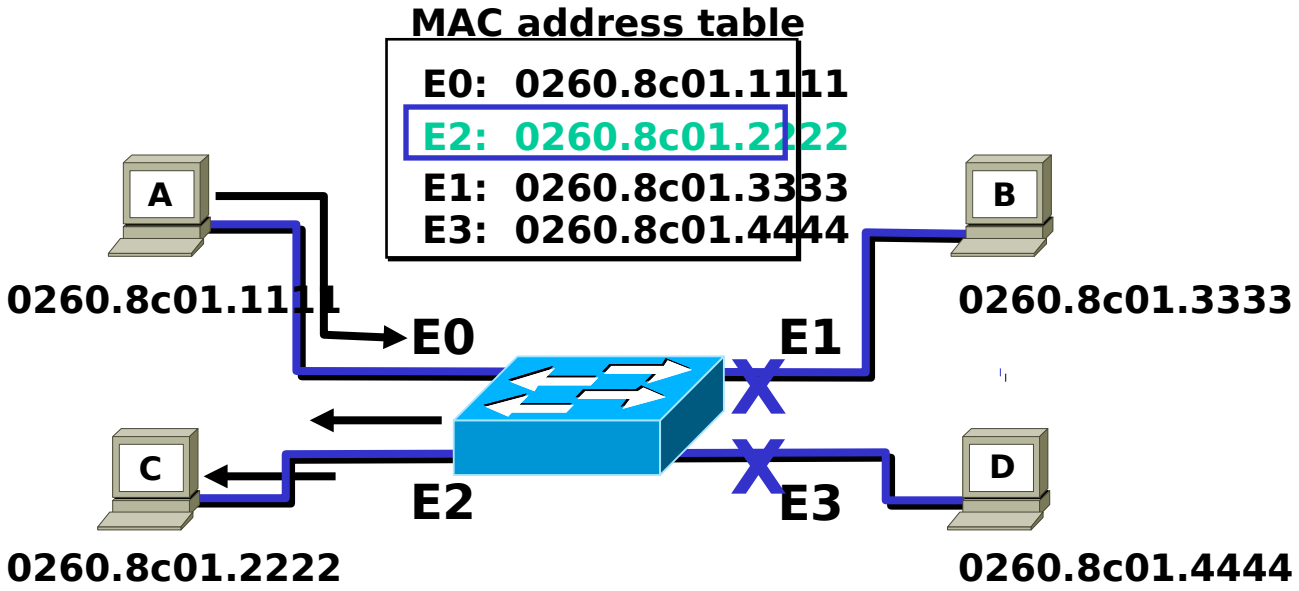
- Break Up Collision Domains
  - Layer 2 Switching is Hardware Based
    - Application-Specific Integrated Circuits (ASICs)
    - No modification to Layer 2 Header
- Provide Segmentation
  - Each Port is a segment
  - Can achieve Gigabit Speeds

Three Main Tasks



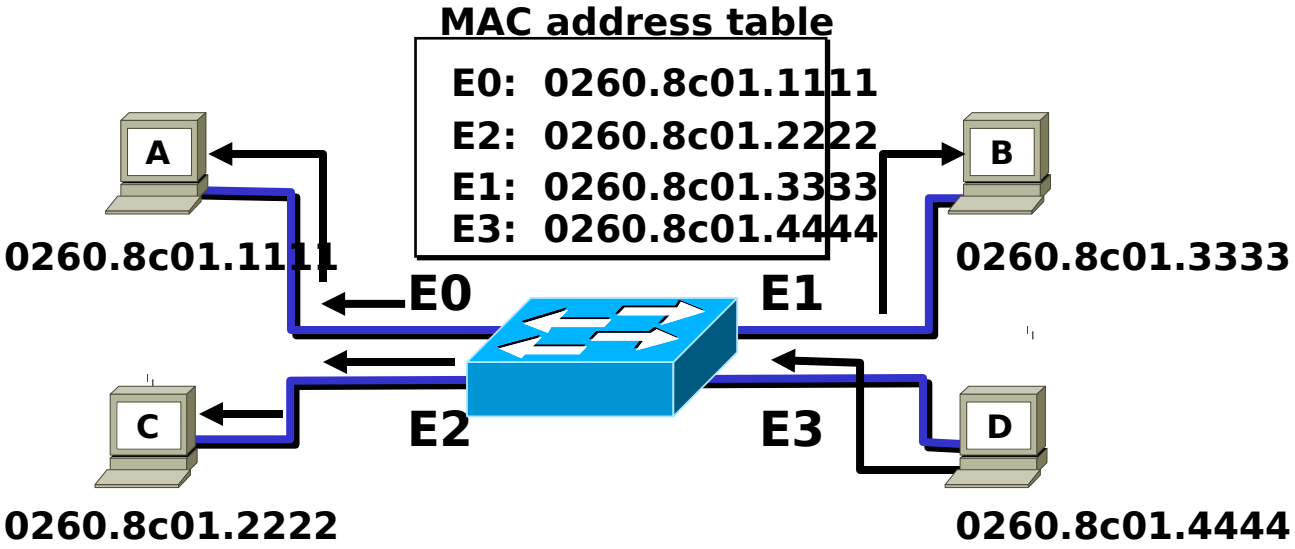
- Address learning
- Forward/filter decision
- Loop avoidance

Filtering Frames



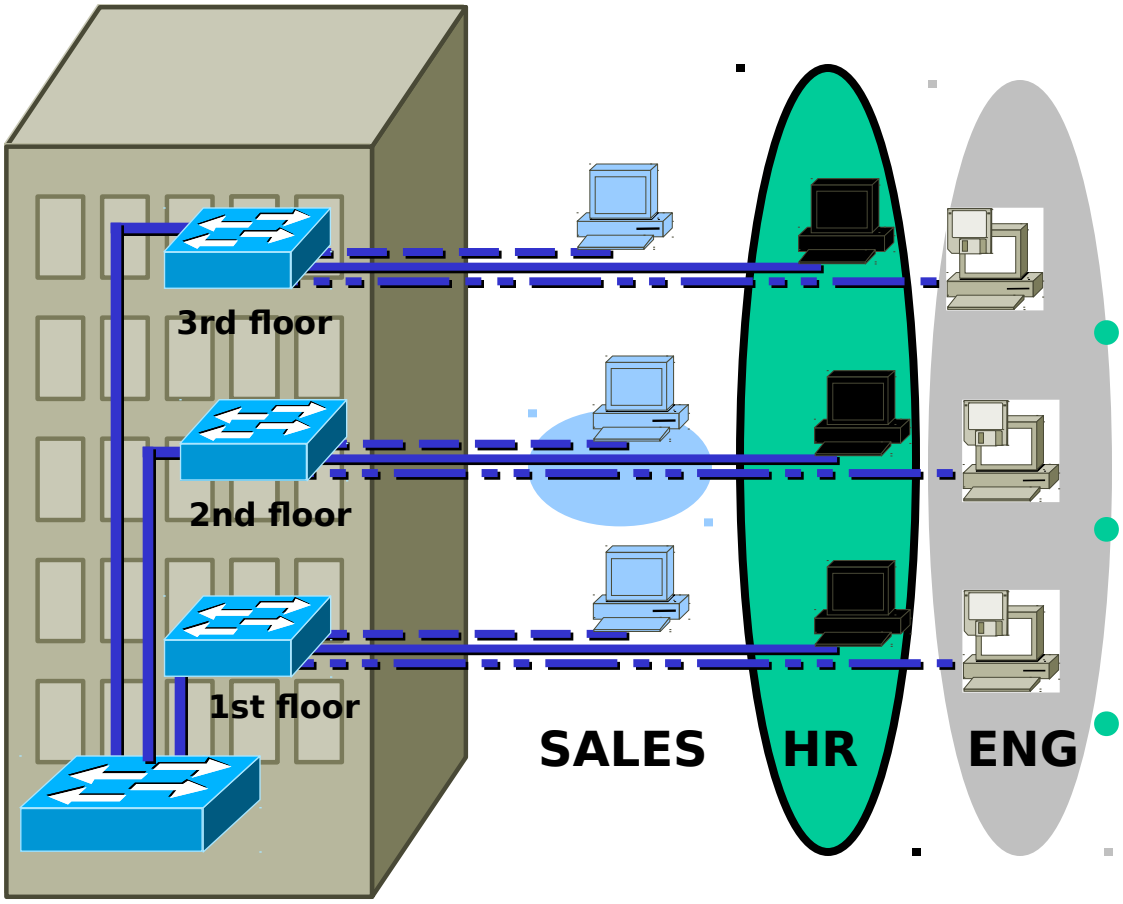
Station A sends a frame to station C
Destination is known, frame is not flooded

Broadcast and Multicast Frames



- **Station D sends a broadcast or multicast frame**
- **Broadcast and multicast frames are flooded to all ports other than the**

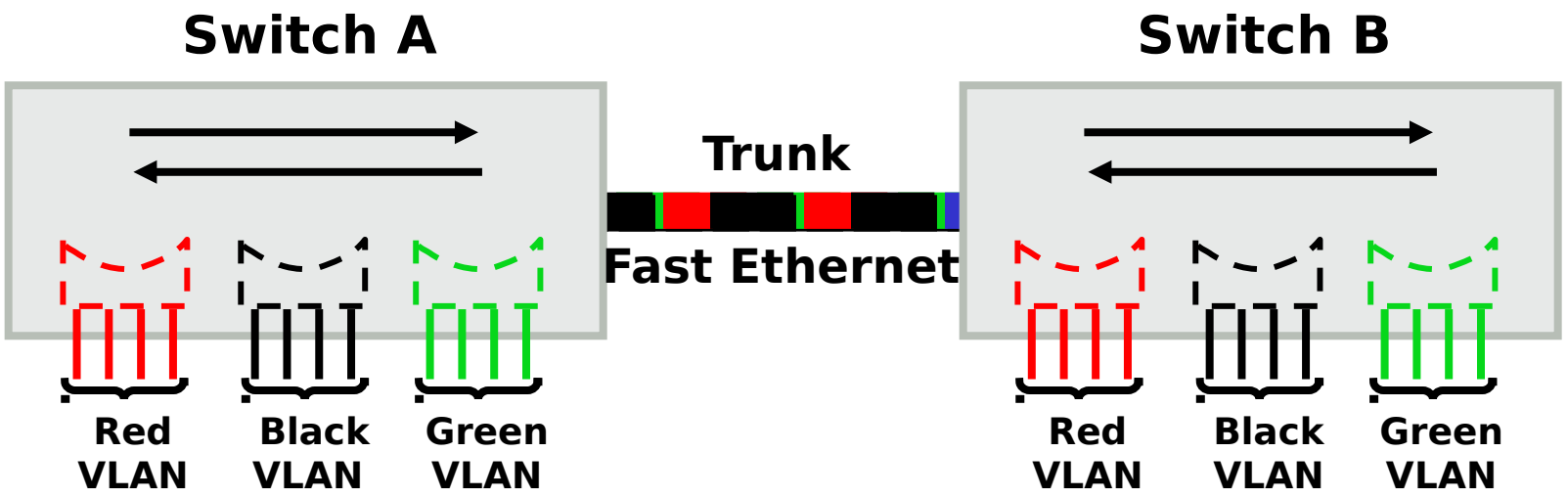
VLAN Overview



- **Segmentation**
- **Flexibility**
- **Security**

VLAN = A broadcast domain = Logical network (subn

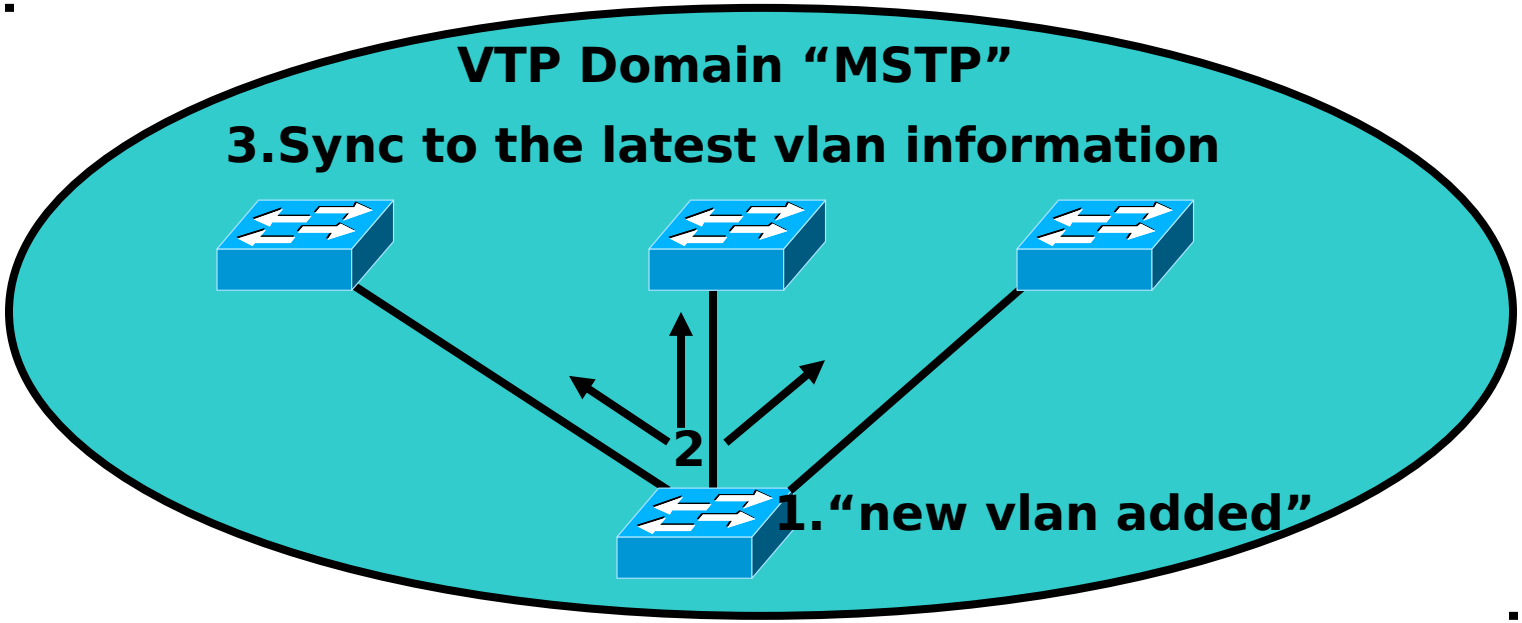
VLAN Operations



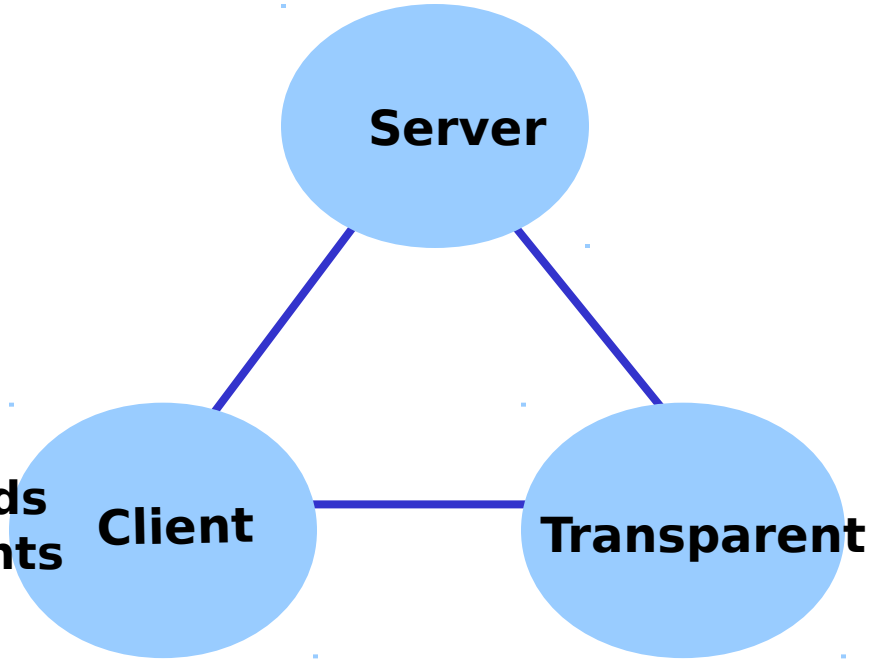
- **Each logical VLAN is like a separate physical bridge**
- **VLANs can span across multiple switches**
- **Trunks carries traffic for multiple VLANs**

VLAN Trunking Protocol (VTP)

- A messaging system that advertises VLAN configuration information
- Maintains VLAN configuration consistency throughout a common administrative domain
- VTP sends advertisements on trunk ports only
- Support mixed media trunks (Fast Ethernet, FDDI, ATM)



VTP Modes



Server Mode
- Create vlans
- Modify vlans
- Delete vlans
- Sends/forwards advertisements
- Synchronize Domain
- Saved in NVRAM

Client Mode
- Sends/forwards advertisements
- Synchronize
- Not saved in NVRAM

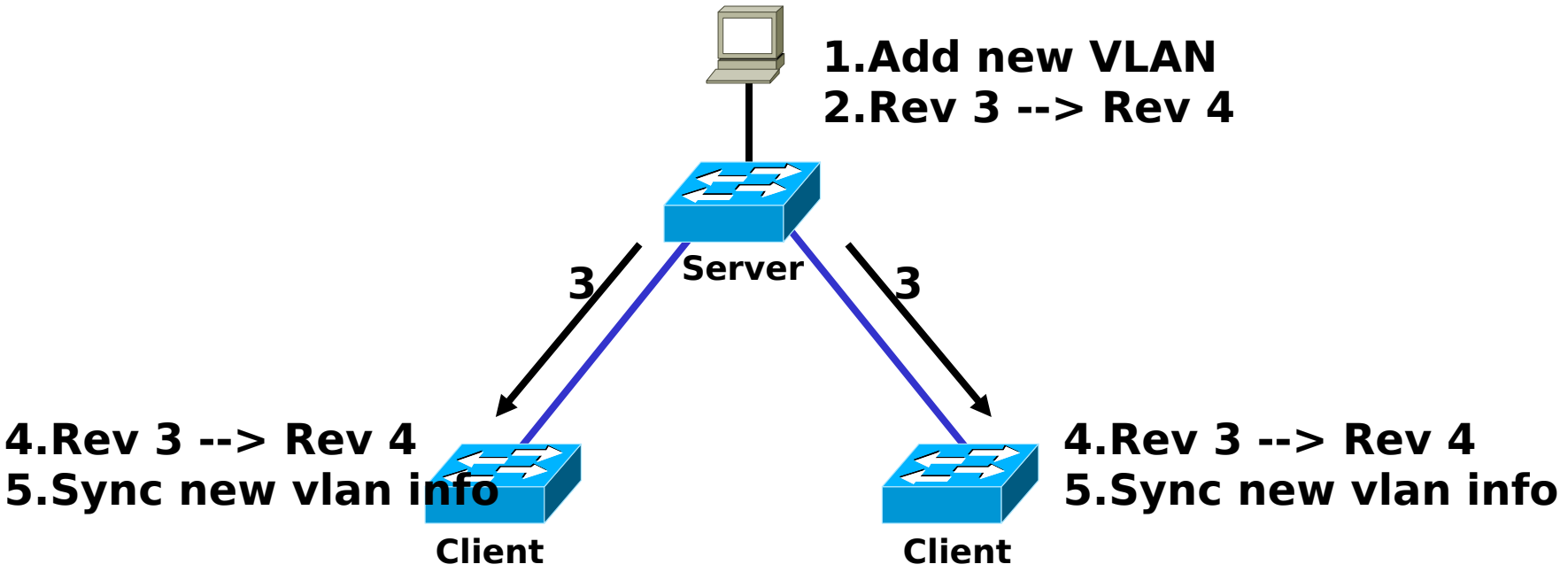
Transparent Mode
- Create vlans
- Modify vlans
- Delete vlans
- Forwards advertisements
- Does not synchronize
- Saved in NVRAM

How VTP Works

VTP advertisements are sent as multicast frames

VTP servers and clients synchronized to latest revision number

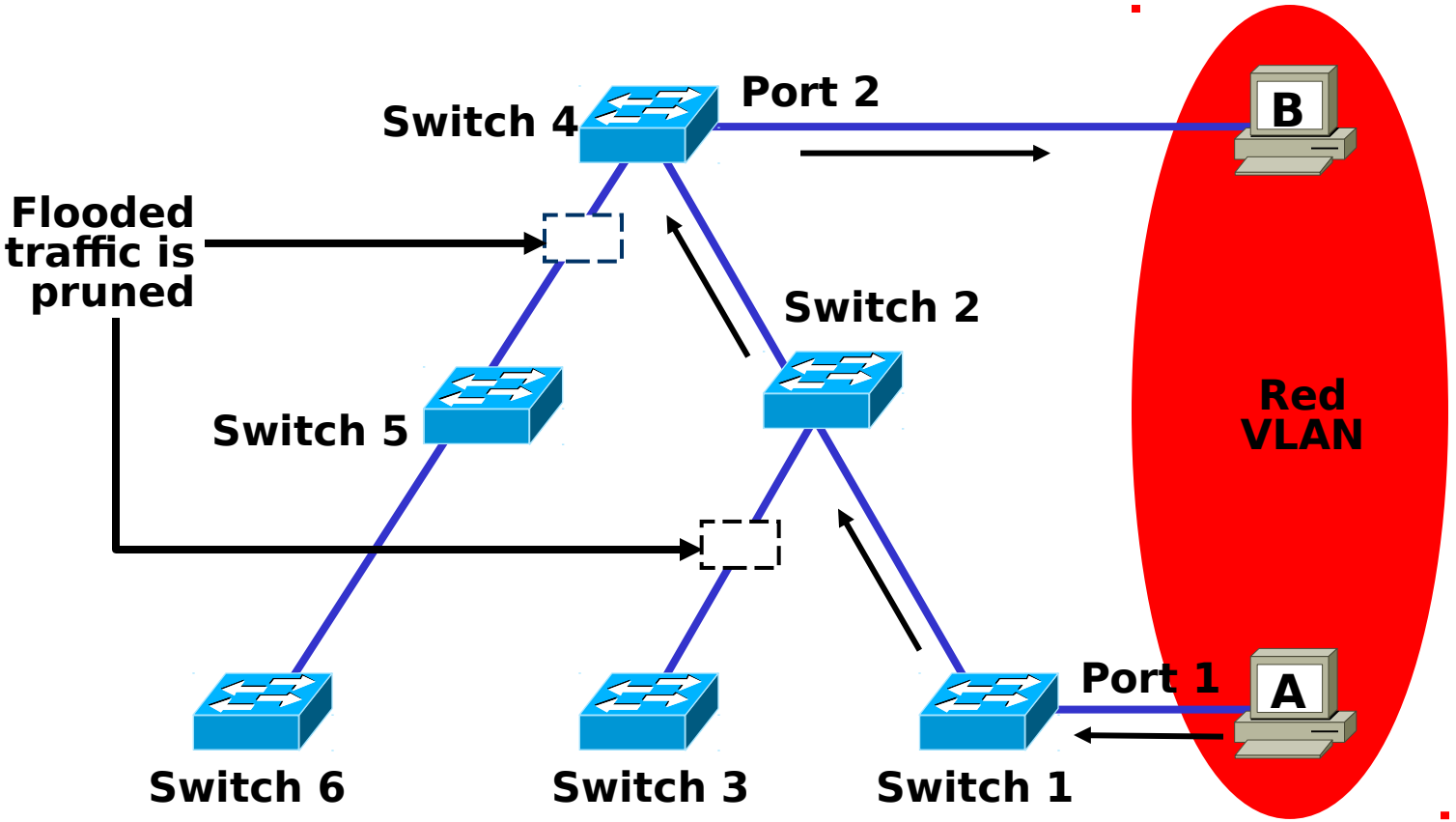
VTP advertisement are sent every five minutes or when there is a change



VTP Pruning

Increases available bandwidth by reducing unnecessary flooded traffic

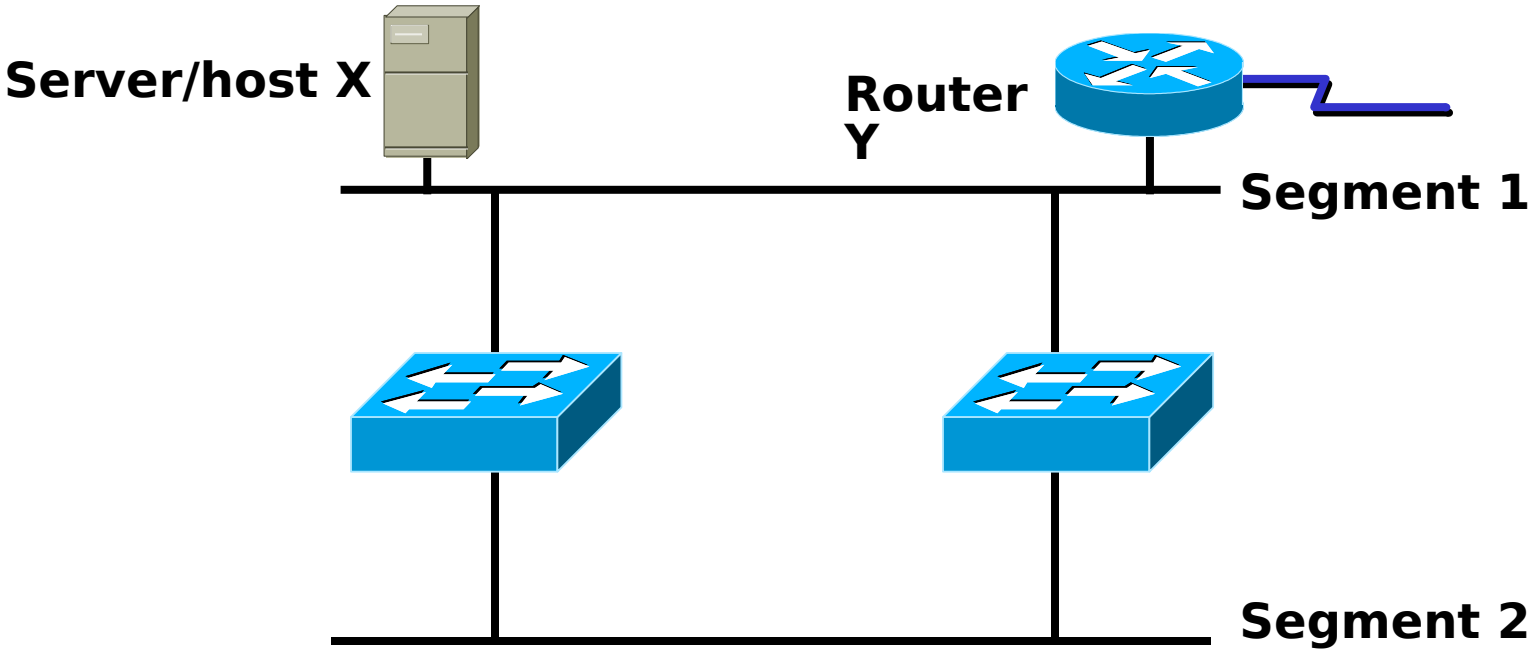
Example: Station A sends a broadcast, broadcast is only flooded to switches that have ports assigned to the red VLAN



VLAN Guidelines

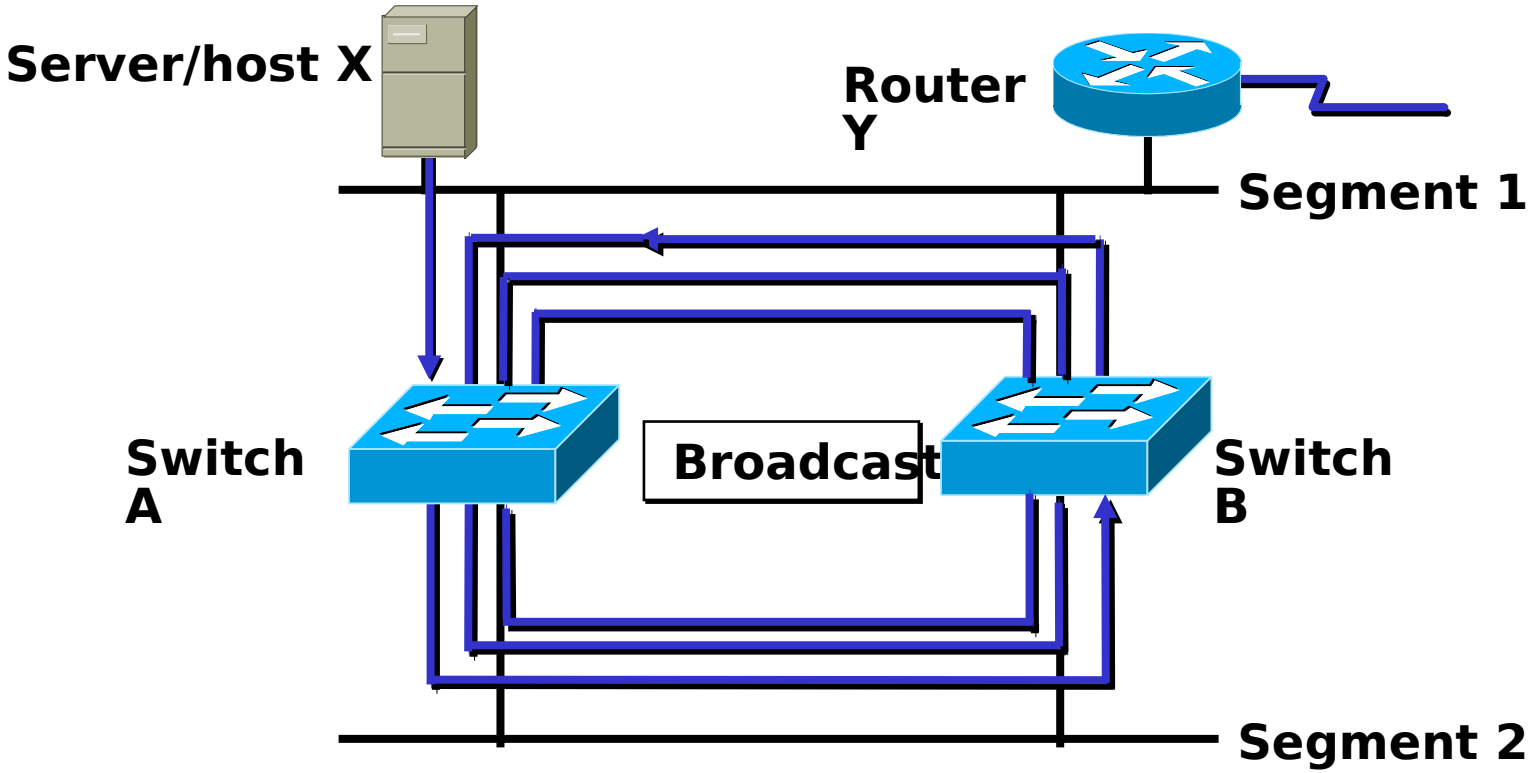
- Maximum number of VLANs, switch-dependent
  - Catalyst 6XXX, 55XX, 35XX, support 1005 VLANS
  - Catalyst 1900 supports 64 VLANs
- 5 Factory Default VLANS
  - VLAN 1 (Can not change VLAN 1 name)
  - VLAN 1001-1005
- CDP and VTP advertisements are sent on VLAN1
  - Must be in VTP server or transparent mode to create, add, or delete VLANs

Redundant Topology



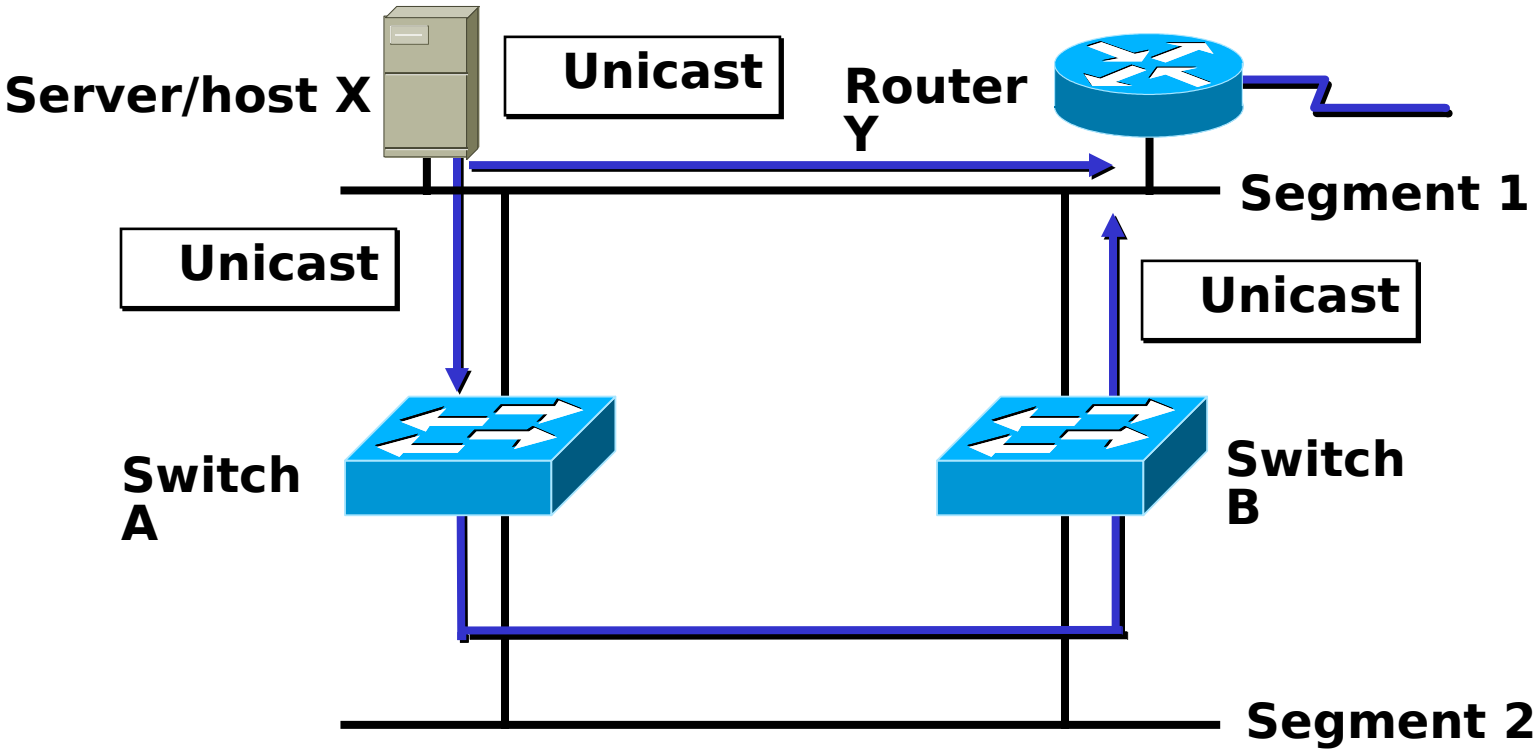
- Redundant topology eliminates single points of failure
- Redundant topology causes broadcast storms, multiple frame copies, and MAC address table instability problems

Broadcast Storms



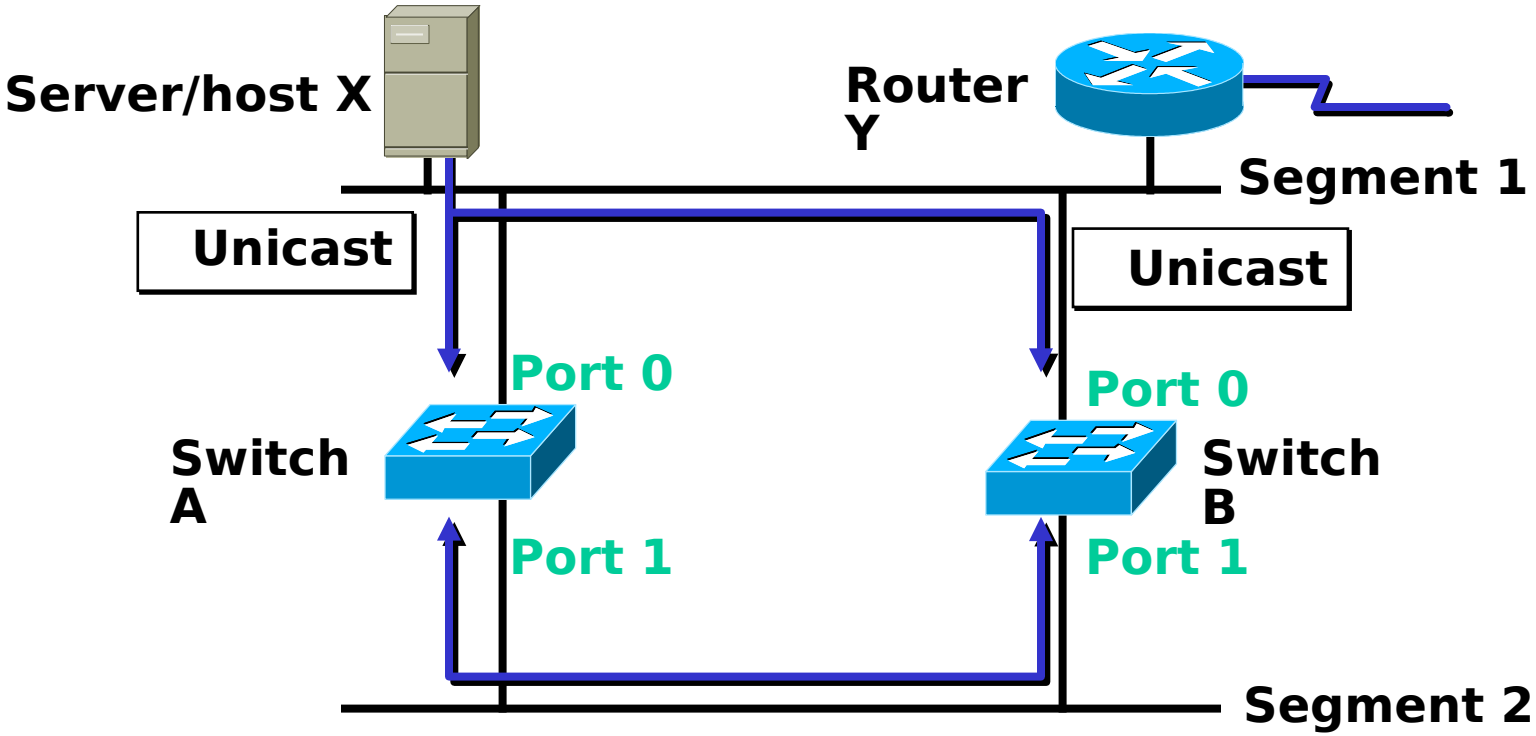
Switches continue to propagate broadcast traffic over and over

Multiple Frame Copies



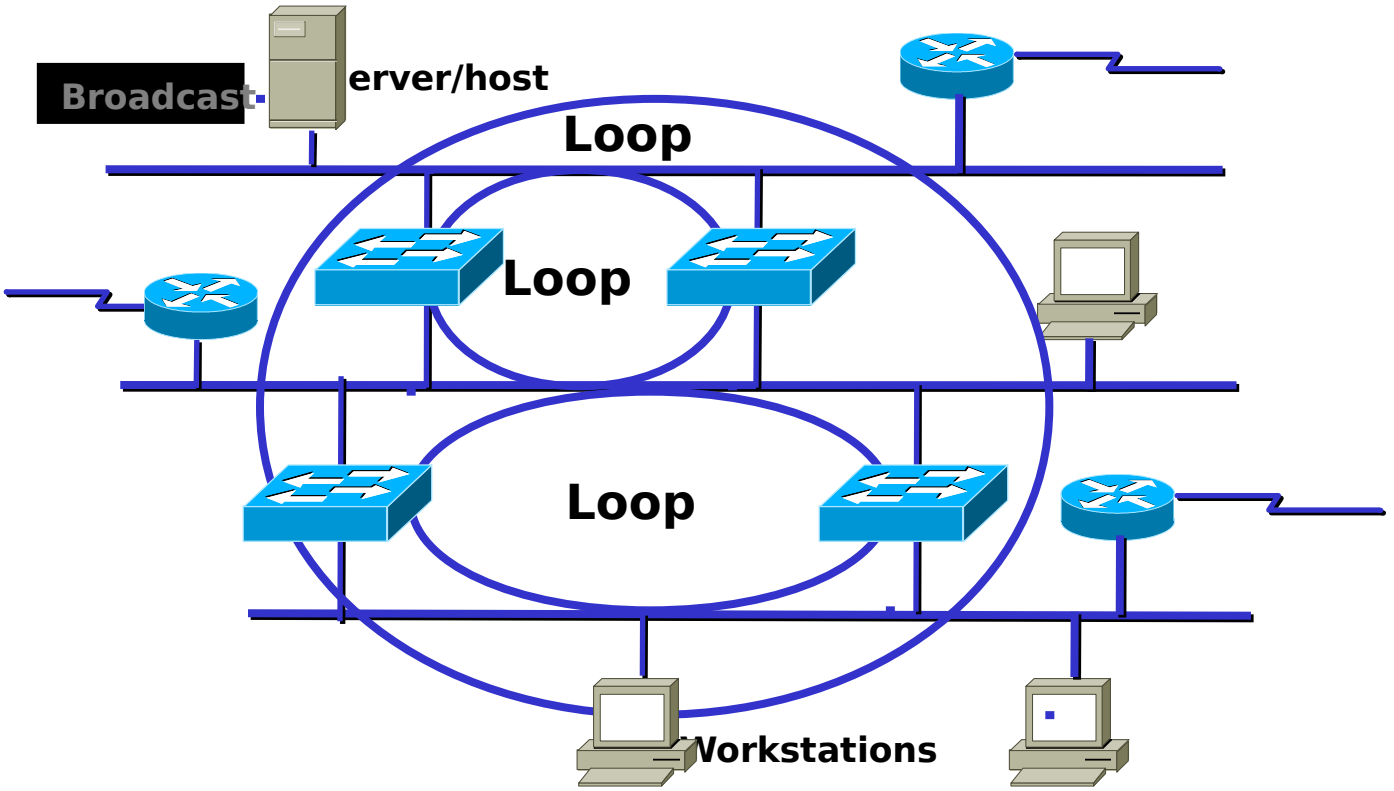
- Host X sends an unicast frame to Router Y
- Router Y MAC Address has not been learned by either Switch yet
- Router Y will receive two copies of the same frame

MAC Database Instability



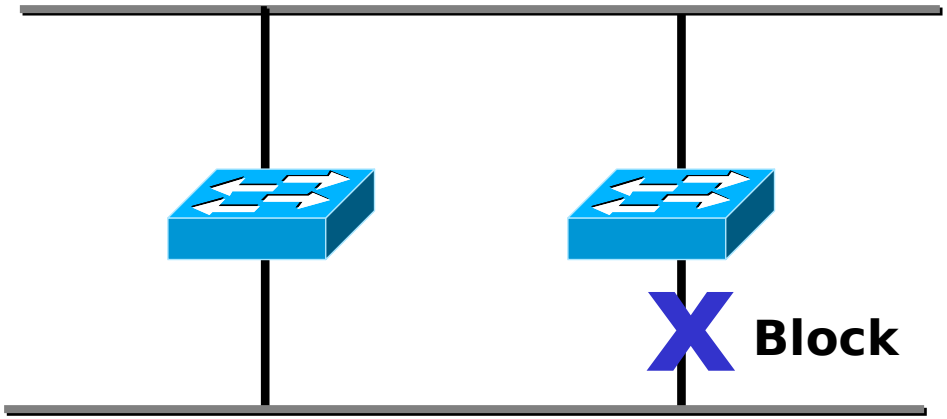
- Host X sends an unicast frame to Router Y
- Router Y MAC Address has not been learned by either Switch y
- Switch A and B learn Host X MAC address on port 0
- Frame to Router Y is flooded
- Switch A and B incorrectly learn Host X MAC address on port 1

Multiple Loop Problems



- Complex topology can cause multiple loops to occur
- Layer 2 has no mechanism to stop the loop

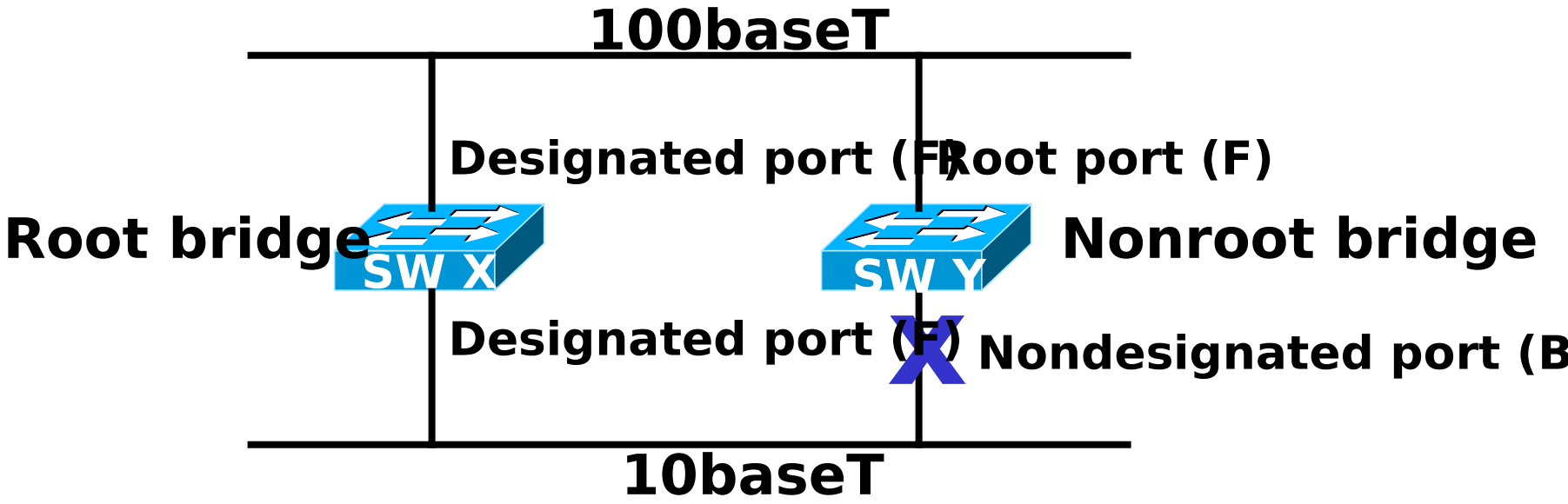
Solution: Spanning-Tree Protocol



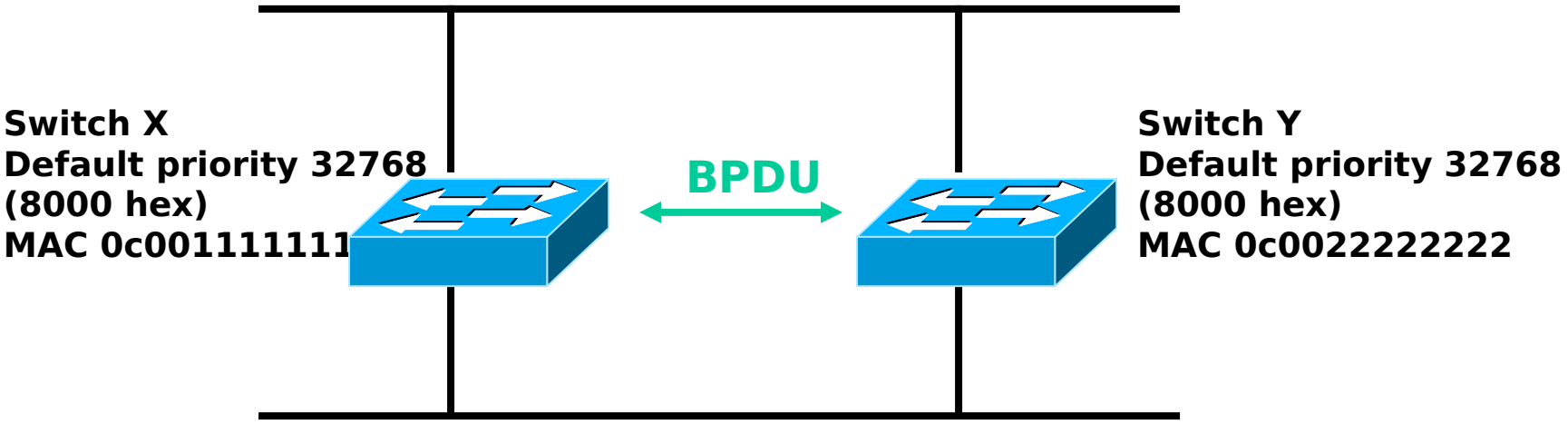
Provides a loop free redundant network topology by placing certain ports in the blocking state

Spanning-Tree Operations

- One root bridge per network
- One root port per nonroot bridge
- One designated port per segment

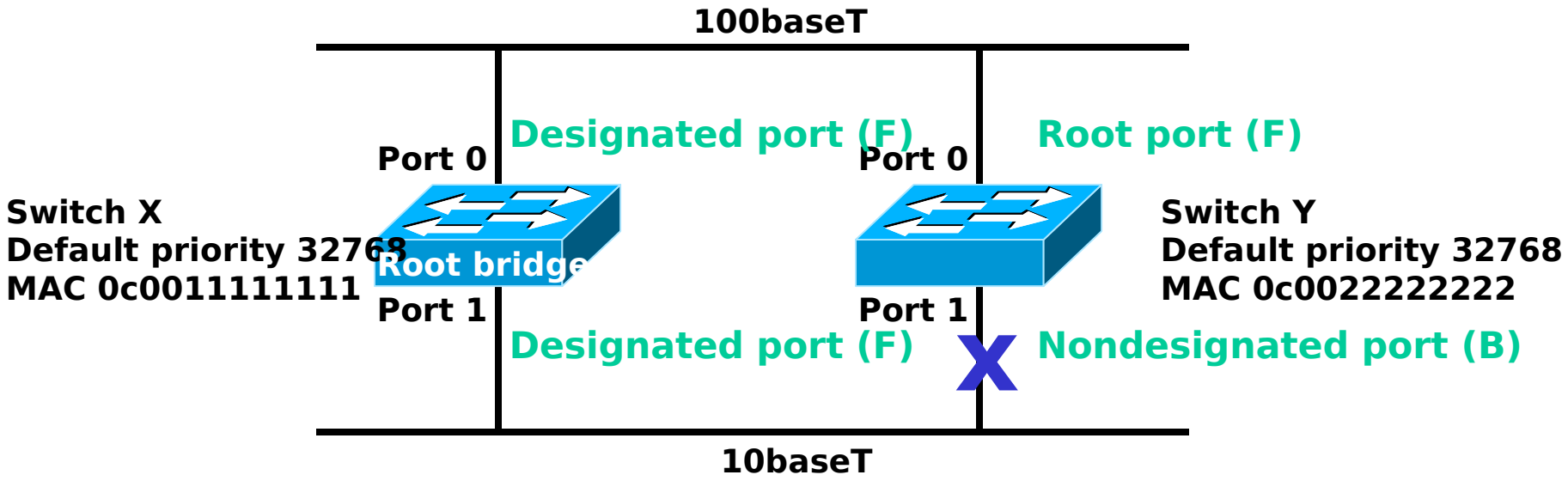


Root Bridge Selection

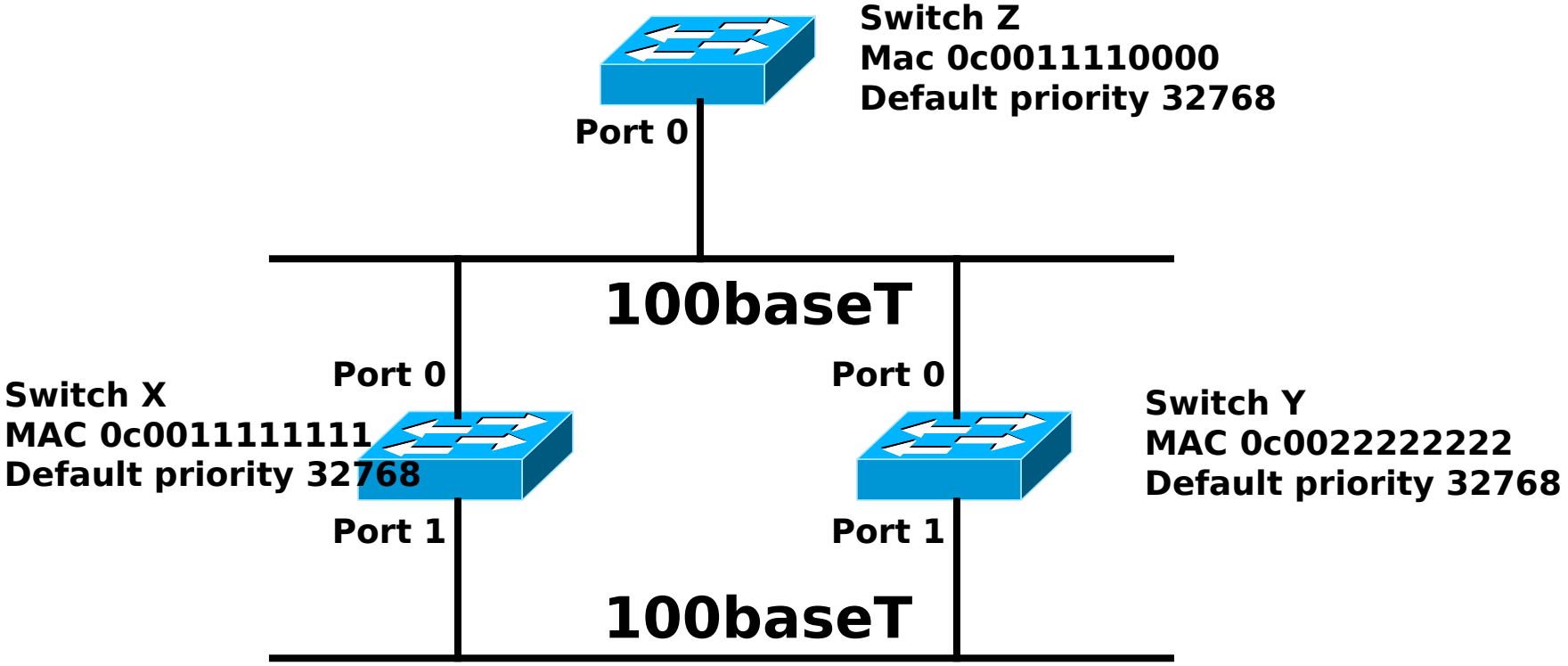


BPDU = Bridge protocol data unit
(default = sent every 2 seconds)
Root bridge = Bridge with the lowest bridge ID
Bridge ID = Bridge priority + bridge MAC address
In the example, which switch has the lowest bridge ID?

Port States


100baseT
Designated port (F)
Root port (F)
Port 0
Port 0
Switch X
Default priority 32768
MAC 0c0011111111
Root bridge
Switch Y
Default priority 32768
MAC 0c0022222222
Port 1
Port 1
Designated port (F)
Nondesignated port (B)
X
10baseT

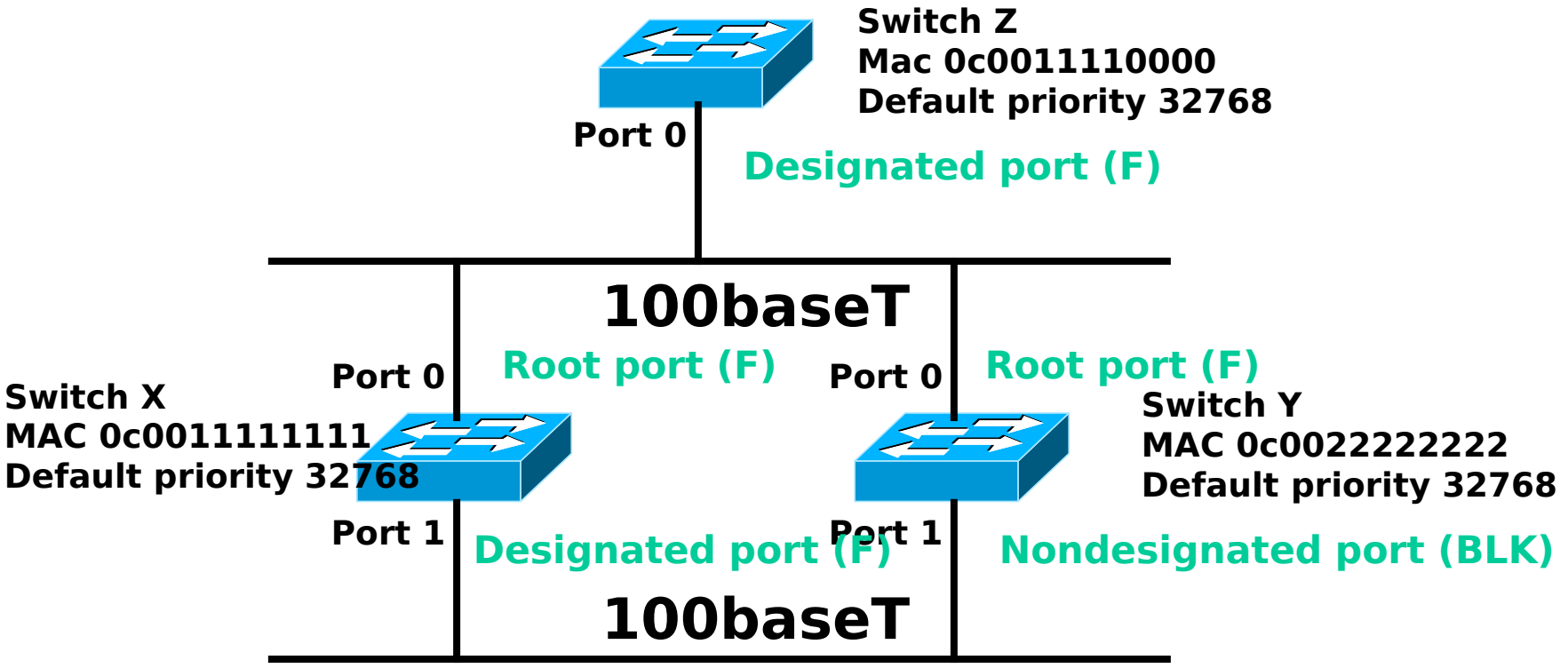
Spanning-Tree



Can you figure out:

- **What is the root bridge?**
- **What are the designated, nondesignated, and root parts?**
- **Which are the forwarding and blocking ports?**

Spanning-Tree



Can you figure out:

- **What is the root bridge?**
- **What are the designated, nondesignated, and root parts?**
- **Which are the forwarding and blocking ports?**